The EU AI Act

Guide for In-House Lawyers

February 2025

HUNTON

Table of Contents

1. Introduction to the AI Act

Regulatory Landscape

Context and Background

Artificial Intelligence ("AI") encompasses a rapidly advancing set of technologies that offer a wide range of economic, environmental, and societal benefits across various industries and social realms. By enhancing prediction capabilities, streamlining operations and resource allocation, and tailoring digital solutions for individuals and businesses, AI can confer significant competitive advantages to businesses and promote positive outcomes in diverse areas such as healthcare, agriculture, food safety, education, media, sports, culture, infrastructure management, energy, transportation, public services, retail, security, and resource efficiency, as well as climate change mitigation and adaptation efforts. Depending on its application, use, and degree of technological advancement, AI also carries with it the potential to pose risks and harm to public interests and fundamental rights protected by EU law.

Given the significant societal impact of AI and the need to foster trust, the EU took steps to develop a regulatory and legal framework that aligns with EU values and takes into account EU fundamental rights and freedoms. The AI Act is the first comprehensive law on AI to be enacted. Like the GDPR, the AI Act is intended to become a global standard.

Objectives of the AI Act

The AI Act aims to enhance the internal market by establishing consistent rules for the development, introduction, and use of AI systems within the EU. It seeks to encourage the adoption of AI that is centered on human values and reliability while safeguarding health, safety, and fundamental rights, including democracy and the rule of law, as well as environmental protection from any adverse impacts of AI systems. Additionally, the AI Act supports innovation. It ensures the unrestricted movement of AI-based products and services across EU borders, preventing EU Member States from imposing limitations on AI system development, marketing, and usage unless explicitly permitted by the AI Act.

Impact on Businesses

The AI Act will significantly change the regulatory and legal framework for AI. The AI Act entered into force on 1 August 2024. Depending on the type of AI system that they use or develop, businesses will have between 6 and 36 months from the entry into force of the AI Act to comply with the applicable obligations. In-house lawyers should urgently consider the impact of the AI Act on their business and plan ahead. Failure to do so could leave businesses with new requirements to implement without having set aside appropriate resources to do so.

Interplay with the GDPR

The GDPR regulates the processing of personal data within the EU but also extends its jurisdiction beyond EU borders, requiring compliance from businesses worldwide processing personal data of individuals located in the EU. Similarly, the AI Act will have global implications, imposing obligations on businesses located outside of the EU, particularly those that place AI systems in the EU market or put the technology into service in the EU. While the GDPR focuses on controllers and processors, the AI Act targets providers, deployers, and users of AI systems.

Businesses should carefully assess the interplay between the two pieces of legislation to determine whether and to what extent they are subject to GDPR and/or AI Act requirements, and also to identify areas where compliance synergies can be leveraged.

The obligation pages in this Guide (Sections 6, 7 and 8 of this Guide) consider the interplay between the obligations introduced by the AI Act and existing obligations under the GDPR. Interplay icons aim to assist in-house lawyers in identifying areas where existing GDPR compliance programs can be leveraged for AI Act compliance. See Section 2 of this Guide for more information on how the icons work.

Interplay with Other Relevant Legislation

Given the expansive reach and transformative potential of AI across diverse sectors and industries, the AI Act will overlap with a multitude of existing EU laws. In-house lawyers will need to carefully factor in such laws when developing and executing their businesses' AI compliance initiatives. This will require a multidisciplinary legal team with expertise in, amongst others, privacy, labour, contract, product liability, consumer protection, market surveillance, and intellectual property law. In order to develop and maintain a practical, risk-based AI compliance program, the legal team will need to work closely together with the other relevant teams within the business, including product development and engineering.

Market Surveillance Rules

Market surveillance rules, particularly those set out in the Accreditation and Market Surveillance Regulation and the Market Surveillance Regulation, govern key elements of the AI Act, such as the conformity assessment procedure and enforcement processes. The interplay between the AI Act and market surveillance rules is discussed in more detail in the sections of this Guide on obligations of providers of high-risk AI systems and enforcement.

Product Liability Directive

The AI Act gives any natural or legal person the right to lodge a complaint with the relevant MSA in case of an infringement. However, unlike the GDPR, the AI Act does not establish rules on liability of providers, deployers, and other agents for breaches of the AI Act vis-à-vis the individual suffering damages. This means that current national rules on tort law and contractual liability will apply. In addition, the new Product Liability Directive came into force on 8 December 2024. The Product Liability Directive replaces the product liability rules currently applicable in the EU and adapts the legal framework to the emergence of new technologies such as AI. This legal instrument is particularly relevant for providers, as they will frequently be considered producers under the Product Liability Directive. Member States have until 9 December 2026 (24 months) to transpose the Product Liability Directive into their national legal frameworks.

AI Liability Directive

In addition to the Product Liability Directive, the EU is also discussing the implementation of a specific framework governing tort liability for damages caused by AI, i.e., the AI Liability Directive. The legislative proposal is still at an early stage, but it intends to facilitate the disclosure of evidence and establishment of the causal link necessary to support claims for damages caused by an AI system. If approved in its current form, the AI Liability Directive would allow providers to rely on their compliance with the applicable provisions of the AI Act as a defence against liability claims.

Cyber Resilience Act and the Cybersecurity Act

On 30 November 2023, the European Institutions reached a political agreement on the text of the Cyber Resilience Act, which introduces new cybersecurity requirements applicable to products with digital elements. The text was approved by the EU Parliament on 12 March 2024 and formally adopted by the Council on 10 October 2024. Providers under the AI Act that also fall within the scope of the EU's Cyber Resilience Act will be able to demonstrate compliance with the cybersecurity requirement of the AI Act by fulfilling the essential cybersecurity requirements set out in the Cyber Resilience Act through an EU declaration of conformity (Recital 77 of the AI Act). Proof of compliance with the AI Act's cybersecurity requirements may also be achieved through a certification system set out under the Cybersecurity Act (Recital 122 and Article 42 of the AI Act). Considering the broad scope of the Cyber Resilience Act, providers should carefully consider if their AI systems fall under the two sets of rules and leverage existing synergies.

Digital Services Act

Risk management rules under the AI Act will interact with the risk management rules applicable under the Digital Services Act, particularly for very large online platforms and very large online search engines. In some cases, these entities may enjoy a presumption of conformity with certain provisions of the AI Act if they follow equivalent provisions under the Digital Services Act (Recital 118 of the AI Act) and may leverage their AI Act compliance measures to support Digital Services Act compliance and vice-versa.

Accessibility Directives

Providers of high-risk AI systems must take into consideration, as applicable, the provisions on accessibility requirements of the Accessibility Directives, which impose rules for accessible products and services.

Copyright Directive

Providers of general-purpose AI models should consider the interplay between the AI Act and the EU's Copyright Directive, such as the obligation to put in place a policy to comply with EU copyright law and, in particular, to identify and comply with (including through state-of-the-art technologies) a reservation of rights pursuant to Article 4(3) of the Copyright Directive (Recitals 104-106 and Article 53(1)(c) of the AI Act).

Union Harmonisation Legislation

For providers of high-risk AI systems under Annex I of the AI Act (see Section 5 of this Guide), there may be specific simplified compliance rules, for example, as regards to the conformity assessment procedure (see page 39 of this Guide). In-house lawyers should carefully consider whether their high-risk AI systems fall within the scope of Annex I of the AI Act and, if so, whether they can benefit from simplified compliance rules and/or are subject to different obligations as a result.

Areas Left Unharmonised by the AI Act

Some areas remain untouched by the AI Act and other EU legislation. Businesses should identify and consider additional relevant laws and regulations at Member State level when developing and implementing their AI compliance measures. For example, the rules around civil liability are mostly non-harmonised and, hence, national tort law and contractual liability rules must be applied.

Member States also have some leeway in establishing penalties and other enforcement measures that will apply in addition to the mandatory fines under the AI Act (see Section 9 of this Guide). Furthermore, the AI Act does not regulate possible criminal liability for misuse of AI systems. As an example, while there are certain transparency obligations applicable to deepfakes (see Section 8 of this Guide), the use of this technology for illegal purposes (e.g., fraud) may be subject to criminal penalties in certain EU Member States.

2. Using this Guide

The purpose of this Guide is to assist in-house lawyers in identifying the impact of the AI Act on their business and developing appropriate practical compliance measures.

The Guide provides an overview of the key topics of the AI Act that are most likely to affect businesses, focusing on obligations for AI providers and deployers. Each obligation page is structured as follows:

- First, there is a description of the requirements imposed by the AI Act;
- Second, in the practical compliance steps box, there is an explanation of why each topic and obligation matters to businesses and the practical compliance steps that businesses may consider taking in this respect; and
- In the third box, there is an explanation of the interplay between the requirements introduced by the AI Act and existing obligations under the GDPR. Icons indicate areas where existing GDPR compliance programs can be leveraged for AI Act compliance.

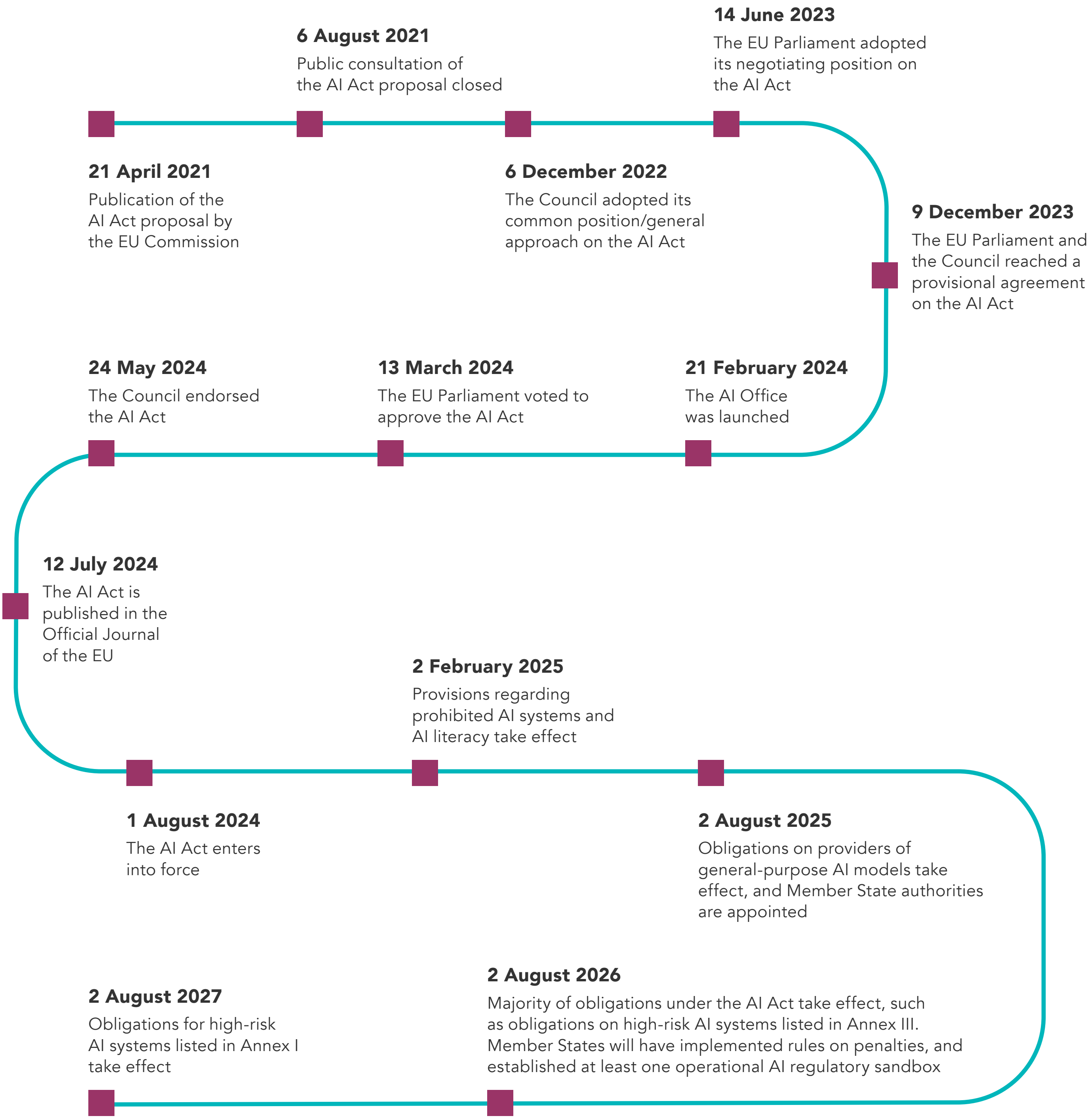
The Guide uses the following icons:

⊕↑	There is substantial overlap with a similar obligation under the GDPR. Minimal efforts will be required to comply with the relevant requirement under the AI Act for businesses that already comply with the corresponding GDPR requirement.
⊖	There is overlap with a GDPR obligation. The measures that have been put in place for GDPR compliance may serve as a starting point for compliance with the AI Act, but adaptations and additional efforts will be required for AI Act compliance.
↓	The obligation under the AI Act is new and does not overlap with an existing obligation under the GDPR. Businesses will not be able to leverage GDPR compliance measures to comply with the relevant requirement under the AI Act.

Defined terms and abbreviations used in this Guide are explained in the Glossary in Section 10.

PLEASE NOTE: This Guide should be used as general guidance only and should not be relied upon as legal advice. You are welcome to re-use the content of this Guide, provided you credit Hunton Andrews Kurth, LLP using the copyright notice set out at the end of this document. For advice on the AI Act and other more detailed questions, please contact Privacy@Hunton.com.

3. Key Dates of the AI Act



21 April 2021
Publication of the AI Act proposal by the EU Commission

6 August 2021
Public consultation of the AI Act proposal closed

6 December 2022
The Council adopted its common position/general approach on the AI Act

14 June 2023
The EU Parliament adopted its negotiating position on the AI Act

9 December 2023
The EU Parliament and the Council reached a provisional agreement on the AI Act

21 February 2024
The AI Office was launched

13 March 2024
The EU Parliament voted to approve the AI Act

24 May 2024
The Council endorsed the AI Act

12 July 2024
The AI Act is published in the Official Journal of the EU

1 August 2024
The AI Act enters into force

2 February 2025
Provisions regarding prohibited AI systems and AI literacy take effect

2 August 2025
Obligations on providers of general-purpose AI models take effect, and Member State authorities are appointed

2 August 2026
Majority of obligations under the AI Act take effect, such as obligations on high-risk AI systems listed in Annex III. Member States will have implemented rules on penalties, and established at least one operational AI regulatory sandbox

2 August 2027
Obligations for high-risk AI systems listed in Annex I take effect

4. Scope of the AI Act

Territorial Scope (Article 2)

The territorial applicability of the AI Act will be determined by three criteria:

Where…	
…an entity is established or located	The AI Act is applicable to deployers that have their place of establishment or who are located within the EU (Article 2(1)(b) of the AI Act).
…the AI system or model is placed on the market or put into service	The AI Act applies to: (i) providers placing AI systems on the market or putting them into service, or placing general-purpose AI models on the market in the EU, irrespective of whether those providers are established or located within the EU or in a third country (Article 2(1)(a) of the AI Act); (ii) importers and distributors importing or distributing the AI system on the EU market (Article 2(1)(d) of the AI Act); and (iii) product manufacturers placing on the market or putting into service an AI system under their own name or trademark (Article 2(1)(e) of the AI Act) in the EU.
…the output of the AI system is used	The AI Act applies to: (i) providers and deployers of AI systems where the output of the system is used in the EU, regardless of where they are established or located (Article 2(1)(c) of the AI Act); and (ii) persons affected by the use of an AI system that are located in the EU (Article 2(1)(g) of the AI Act).

The AI Act will also apply to authorised representatives of providers who are not established in the EU (Article 2(1)(f).

Personal and Material Scope (Article 2)

The AI Act mainly targets providers and deployers of AI systems (see Section 5 of this Guide for definitions). There are limited circumstances where the rules under the AI Act also apply to other parties, such as importers, distributors and product manufacturers.

There are, however, several exceptions. Amongst others, the AI Act does not apply to:

- Deployers who are natural persons and are using the AI systems purely for personal, non-professional activity (Article 2(10) of the AI Act);
- AI systems and models specifically developed and put into service solely for scientific research and development purposes (Article 2(6) of the AI Act); and
- Any research, testing, and development activity regarding AI systems or models prior to being placed on the market or put into service, except for testing in real-world conditions (Article 2(7) of the AI Act).

There are also broad derogations for high-risk AI systems that fall within the scope of the Union Harmonisation Legislation listed in Section B of Annex I of the AI Act (Article 2(2) of the AI Act).

Product manufacturers of high-risk AI systems that are safety components of products covered by Union Harmonisation Legislation listed in Section A of Annex I of the AI Act may also be considered to be the provider of the high-risk AI systems under certain circumstances, including where:

- The high-risk AI system is placed on the market 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 25(3) of the AI Act).

Finally, it is worth noting that any deployer, distributor, importer, or other third party may be considered as a provider when:

- They put their name or trademark on a high-risk AI system already placed on the market or put into service without putting in place contractual arrangements that stipulate that the obligations are allocated otherwise;
- They make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service and it remains a high-risk AI system; or
- They modify the intended purpose of an AI system, including a general-purpose AI model, which has originally not been classified as high-risk and has already been placed on the market or put into service in such manner that the AI system becomes high-risk (Article 25(1) of the AI Act).

The decision trees in Section 5 will help in understanding whether a business should be considered a deployer or a provider under the AI Act.

Temporal Scope (Article 113)

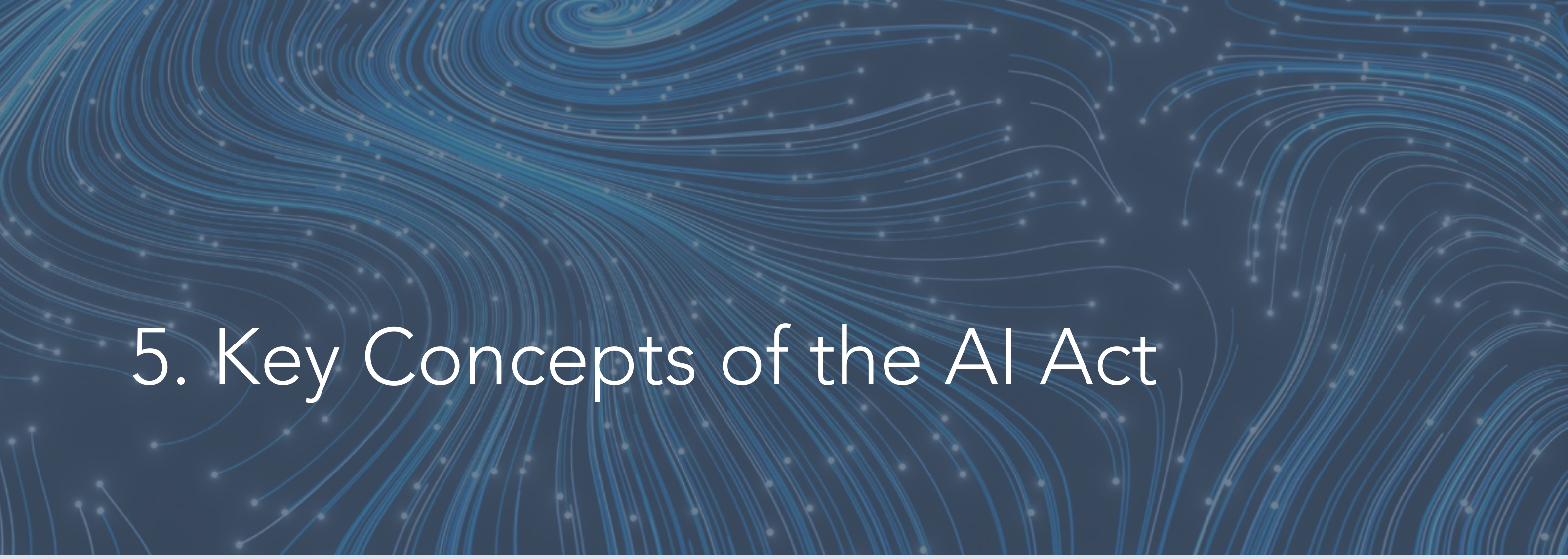
The AI Act will become applicable to regulated entities in stages, following a transition period after the date of entry into force of the AI Act. The length of the transition period will vary depending on the type of AI system:

6 months for the obligations applicable to prohibited AI systems and the obligations related to AI literacy **2 February 2025**	**12 months** for specific obligations applicable to general-purpose AI models **2 August 2025**	**24 months** for most other obligations, including the rules applicable to high-risk AI systems included in Annex III of the AI Act and AI systems subject to transparency requirements **2 August 2026**	**36 months** for the obligations related to high-risk AI systems included in Annex I of the AI Act **2 August 2027**

The AI Act will only apply to high-risk AI systems that have been placed on the market or put into service before 2 August 2026, when those systems have, as from that date, been subject to "significant changes in their designs". More regulatory guidance is expected on what should be considered "significant design changes", including whether updates or training with new datasets would fall within scope.

Providers of general-purpose AI models that have been placed on the market before 2 August 2025 will have until 2 August 2027 to bring them into compliance with the requirements of the AI Act.

Specific timelines also apply to AI systems that are components of large-scale IT systems established in accordance with the legal instruments referred to in Annex X of the AI Act (Article 111(1) of the AI Act).



5. Key Concepts of the AI Act

Key Definitions

Article 3 of the AI Act contains 68 defined terms. Below is a selection of key definitions frequently referenced in this Guide. Some concepts, such as "provider" and "deployer", are further explained in the text of this Guide. Additional terms and abbreviations used in this Guide are defined in the Glossary (see Section 10).

AI SYSTEM means 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. On 6 February 2025 the EU Commission published guidelines further developing the definition of AI system under the AI Act.

GENERAL-PURPOSE AI MODEL means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development, or prototyping activities before they are placed on the market.

GENERAL-PURPOSE AI SYSTEM means an AI system that is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems.

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.

REASONABLY FORESEEABLE MISUSE means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems, including other AI systems.

MAKING AVAILABLE ON THE MARKET means the supply of an AI system or a general-purpose AI model for distribution or use on the EU market in the course of a commercial activity, whether in return for payment or free of charge.

PLACING ON THE MARKET means the first making available of an AI system or a general-purpose AI model on the EU market.

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.

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 rights; or (d) serious harm to property or the environment.

Types of AI Systems

Introduction

The AI Act introduces a risk-based legal framework that imposes more or less stringent requirements depending on the level and type of risks related to the use of the AI system. The AI Act establishes the following types of AI systems: (i) prohibited AI systems; (ii) high-risk AI systems; (iii) systems with transparency requirements; and (iv) general-purpose AI models. This section along with the decision trees provided in the next pages aims to assist in-house lawyers in categorising their AI systems under the AI Act. It is important to note that the different types of AI systems listed below are not mutually exclusive. For example, a high-risk AI system may also be subject to transparency requirements.

Prohibited AI Systems

Prohibited AI systems are AI systems and/or AI uses that have been deemed unacceptable from a fundamental rights perspective and that are, therefore, prohibited:

Subliminal, Purposefully Manipulative, or Deceptive Techniques

(Article 5(1)(a))

AI systems/models that use subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques and that aim at or result in materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing a person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person, or group of persons significant harm. Recital 29 clarifies that this includes AI systems that deploy subliminal components, such as audio, image, video stimuli, or other manipulative or deceptive techniques, that subvert or impair a person's autonomy, decision-making or free choice.

Exploitation of Vulnerabilities

(Article 5(1)(b))

AI systems that exploit a person's or a specific group of persons' vulnerabilities due to their age, disability, or a specific social or economic situation and that aim at or result in materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm. For example, an AI system that is able to assess someone's economic situation and offer disadvantageous loans at moments of particular vulnerability (e.g., a major expense is due) would be prohibited under this provision.

AI Systems Used for Social Scoring

(Article 5(1)(c))

AI systems used to evaluate or classify natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics. The social scoring must lead to: (i) detrimental or unfavourable treatment of certain natural persons or whole groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected; and/or (ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity. For example, an AI system that restricts access to certain public amenities based on the fact that a person protested against government policies would be prohibited under this provision.

AI Systems Used for Predictive Policing

(Article 5(1)(d))

AI systems used for making risk assessments of natural persons in order to assess or predict the likelihood of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics. Based on this prohibition, EU courts cannot, for example, rely on an AI system to calculate the likelihood of recidivism or the likelihood of a defendant fleeing before their court date.

This prohibition does not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity.

AI Systems Used to Build Facial Recognition Databases

(Article 5(1)(e))

AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.

Emotion Inference in the Workplace or Education Institutions

(Article 5(1)(f))

AI systems used to infer emotions of a natural person in the workplace and education institutions. For example, an AI system used to assess whether students are distracted or nervous in classes would be prohibited under this provision. This prohibition does not apply where the AI system is used for medical or safety reasons.

Biometric Categorisation Based on Sensitive Data

(Article 5(1)(g))

AI systems that individually categorise natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation. Under this provision it would, for example, not be permissible to create an AI system that infers someone's race based on facial characteristics.

This prohibition does not apply to any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement. Under this exception, law enforcement authorities may, for example, sort images of individuals based on eye or hair colour (Recital 30 of the AI Act).

Real-time Biometric Identification in Public by Law Enforcement

(Article 5(1)(h))

The use of real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement (e.g., CCTV systems capable of identifying and following a suspect in real time).

This prohibition does not apply to the use of 'real-time' remote biometric identification systems for the purposes established in subparagraphs i) to iii) of Article 5(1)(h) of the AI Act, when the law enforcement authorities comply with the rules under Article 5(2-4) of the AI Act.

On 4 February 2025 the EU Commission published its guidelines on prohibited artificial intelligence practices, further developing the prohibitions established by the AI Act.

High-risk AI Systems

High-risk AI systems are deemed to present a potentially high risk to the rights and freedoms of individuals and are subject to stringent obligations. The AI Act differentiates between two buckets of high-risk AI systems:

EU Harmonisation Legislation

(Article 6(1) and Annex I)

An AI system in this category will be considered high-risk when: (i) it is intended to be used as a safety component of a product, or the AI system is itself a product covered by the EU harmonisation legislation identified in Annex I of the AI Act; and (ii) the product or system has to undergo a third-party conformity assessment under applicable EU harmonisation legislation. This may cover AI systems used in, for example, machinery, toys, lifts, equipment, and safety components for use in medical devices and in vitro diagnostic medical devices, civil aviation-related products, marine equipment, rail system-related products, and various types of vehicles.

Other High-risk AI Systems

(Article 6(2-3) and Annex III)

Annex III of the AI Act lists AI systems as high-risk by direct reference. However, there is an exception to this classification: AI systems listed in Annex III will not be considered high-risk if they do not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons. This is the case when the AI system is intended to: (i) perform a narrow procedural task; (ii) improve the result of a previously completed human activity; (iii) detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or (iv) perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III of the AI Act. AI systems that perform profiling of natural persons may not benefit from these exemptions. Providers who want to rely on one of those exemptions must document their assessment and make it available to competent authorities on request. The registration obligation under Article 49(2) of the AI Act will, however, remain applicable.

High-risk AI systems identified in Annex III of the AI Act include:

- Biometrics (except for AI systems intended to be used for biometric verification that have as their sole purpose to confirm that a specific individual is the person they claim to be) (Annex III(1) of the AI Act), including:
    - Remote biometric identification systems;
    - 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; and
    - Emotion recognition AI systems.
- Critical infrastructure (Annex III(2) of the AI Act), including 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.
- Education and vocational training (Annex III(3) of the AI Act), including AI systems intended to be used to:
    - Determine the access, admission, or assignment to educational and vocational training institutions at all levels;
    - Evaluate learning outcomes;
    - Assess the appropriate level of education that an individual will receive or will be able to access; or
    - Monitor and detect prohibited behaviour of students during tests.
- Employment, workers management, and access to self-employment (Annex III(4) of the AI Act), including AI systems intended to be used to:
    - Recruit or select individuals, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates; or
    - Make decisions affecting terms of work-related relationships, the promotion, or termination of work-related relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.
- Access to and enjoyment of essential private services and essential public services and benefits (Annex III(5) of the AI Act), including AI systems intended to be used:
    - By public authorities or on behalf of 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 and services;
    - To evaluate the creditworthiness of individuals or establish their credit score, except for AI systems used to detect financial fraud;
    - For risk assessment and pricing in relation to individuals in the case of life and health insurance; or
    - To evaluate and classify emergency calls by individuals or to be used to dispatch, or to establish priority in the dispatching of, emergency first response services, including by police, firefighters, and medical aid, as well as of emergency healthcare patient triage systems.

- Law enforcement (Annex III(6) of the AI Act), including AI systems intended to be used by or on behalf of law enforcement authorities, or by EU institutions, bodies, offices, or agencies in support of law enforcement authorities:
    - To assess a natural person's risk of becoming the victim of criminal offences;
    - As polygraphs or similar tools;
    - To evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;
    - To assess the likelihood of an individual offending or reoffending not solely based on profiling of natural persons pursuant to the Law Enforcement Directive, or to assess personality traits and characteristics or past criminal behaviour of individuals or groups; or
    - For the profiling of individuals, as referred to in the Law Enforcement Directive, in the course of the detection, investigation, or prosecution of criminal offences.
- Migration, asylum, and border control management (Annex III(7) of the AI Act), including AI systems intended to be used by or on behalf of competent public authorities or by EU institutions, bodies, offices, or agencies:
    - As polygraphs and similar tools;
    - To assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by an individual who intends to enter or who has entered into the territory of a Member State;
    - To assist competent public authorities for the examination of applications for asylum, visa, or residence permits and for associated complaints with regard to the eligibility of the individuals applying for a status, including related assessments of the reliability of evidence; and
    - In the context of migration, asylum, or border control management, for the purpose of detecting, recognising or identifying individuals, with the exception of the verification of travel documents.
- Administration of justice and democratic processes (Annex III(8) of the AI Act), including AI systems intended to be used:
    - By a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution; and
    - To influence the outcome of an election or referendum or the voting behaviour of individuals in elections or referenda, except for AI systems where individuals are not directly exposed to the output, such as tools used to organise, optimise, or structure political campaigns from an administrative or logistical point of view.

Systems with Transparency Requirements

AI systems with transparency requirements pose specific transparency risks or may mislead end-users due to their nature. The AI Act requires providers and deployers to comply with specific transparency rules designed to mitigate those risks.

Systems with Transparency Requirements

(Article 50)

Article 50 of the AI Act lists the types of AI systems that are subject to transparency requirements due to their nature. Note, this list includes some AI systems that may also be also categorised as high-risk AI systems:

- AI systems intended to interact directly with individuals (Article 50(1) of the AI Act);
- AI systems, including general-purpose AI systems, generating synthetic audio, image, video, or text content (Article 50(2) of the AI Act);
- Emotion recognition systems (Article 50(3) of the AI Act);
- Biometric categorisation systems (Article 50(3) of the AI Act);
- AI systems that generate or manipulate image, audio, or video content constituting a deep fake (Article 50(4) of the AI Act); and
- AI systems that generate or manipulate text which is published with the purpose of informing the public on matters of public interest (Article 50(4) of the AI Act).

General-purpose AI Models

Due to their flexibility and versatility, general-purpose AI models are regulated as a separate category of AI systems. Providers of general-purpose AI models are subject to specific obligations, which are described in more detail on page 48 of this Guide.

General-purpose AI Models

(Articles 51 and 52)

A general-purpose AI model is an AI model, trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, including serving as a basis for general-purpose AI systems (Article 3(63) of the AI Act).

The AI Act also identifies and provides rules for general-purpose AI models with systemic risk. A general-purpose AI model will be considered as having a systemic risk: (i) where it has high impact capabilities; or (ii) when it has equivalent impact or capabilities to an AI model with high-impact capabilities (Article 51(1) of the AI Act). The assessment of whether a model has equivalent impact or capabilities should be performed on the basis of the criteria in Annex XIII of the AI Act.

Providers of general-purpose AI models that have high impact capabilities will have to notify the EU Commission without delay and in any event within two weeks after that requirement is met or they become aware that it will be met (Article 52(1) of the AI Act). In this notification, providers may present counter-arguments regarding the decision to consider that their general-purpose AI model presents a systemic risk (Article 52(2) of the AI Act).

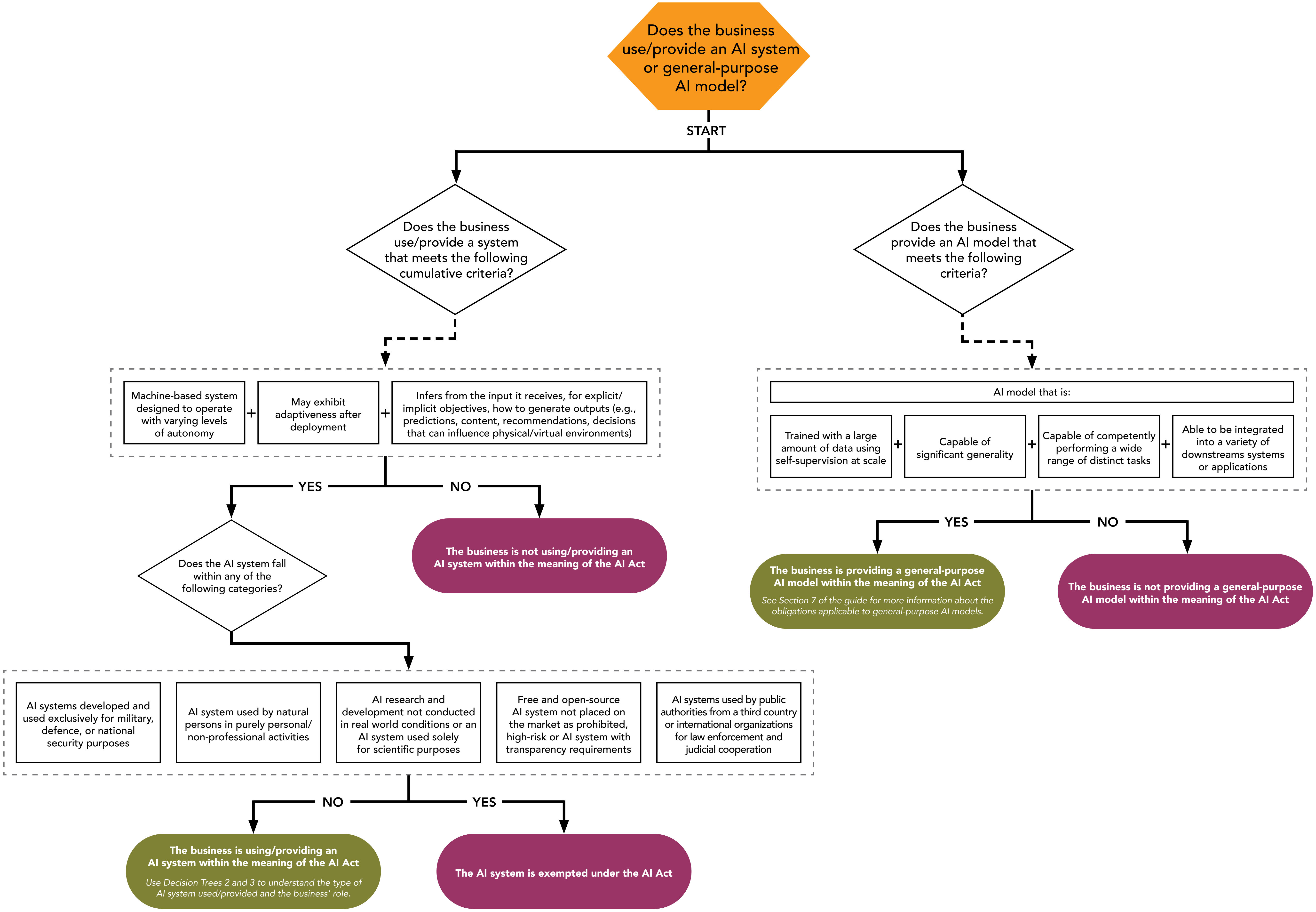
A general-purpose AI model may also be classified as presenting a systemic risk *ex officio* by the EU Commission or following a qualified alert by the scientific panel pursuant to Article 90(1)(a) of the AI Act. A general-purpose AI system will be presumed to have high-impact capabilities when the cumulative amount of computation used for its training is greater than 10^{25} FLOPs (Article 51(2) of the AI Act).

Decision Trees

The following pages contain decision trees—concise, step-by-step visual guides designed to assist in-house lawyers in conducting a preliminary assessment of business exposure to the AI Act. Conclusions drawn from these decision trees should be validated and supplemented by reviewing the rest of this Guide. These tools are intended for joint use and address three main topics:

1. Determining whether a business is using or providing an AI system or general-purpose AI model falling under the scope of the AI Act;
2. Assessing whether the AI system or general-purpose AI model used or provided by the business is subject to obligations under the AI Act; and
3. Identifying whether the business qualifies as a deployer or provider for the purposes of the AI Act.

Decision Tree 1: AI System or General-purpose AI Model



Does the business use/provide an AI system or general-purpose AI model?

START

Does the business use/provide a system that meets the following cumulative criteria?

Machine-based system designed to operate with varying levels of autonomy + May exhibit adaptiveness after deployment + Infers from the input it receives, for explicit/implicit objectives, how to generate outputs (e.g., predictions, content, recommendations, decisions that can influence physical/virtual environments)

YES

Does the AI system fall within any of the following categories?

AI systems developed and used exclusively for military, defence, or national security purposes

AI system used by natural persons in purely personal/non-professional activities

AI research and development not conducted in real world conditions or an AI system used solely for scientific purposes

Free and open-source AI system not placed on the market as prohibited, high-risk or AI system with transparency requirements

AI systems used by public authorities from a third country or international organizations for law enforcement and judicial cooperation

NO

The business is using/providing an AI system within the meaning of the AI Act

Use Decision Trees 2 and 3 to understand the type of AI system used/provided and the business' role.

YES

The AI system is exempted under the AI Act

NO

The business is not using/providing an AI system within the meaning of the AI Act

Does the business provide an AI model that meets the following criteria?

AI model that is:

Trained with a large amount of data using self-supervision at scale + Capable of significant generality + Capable of competently performing a wide range of distinct tasks + Able to be integrated into a variety of downstreams systems or applications

YES

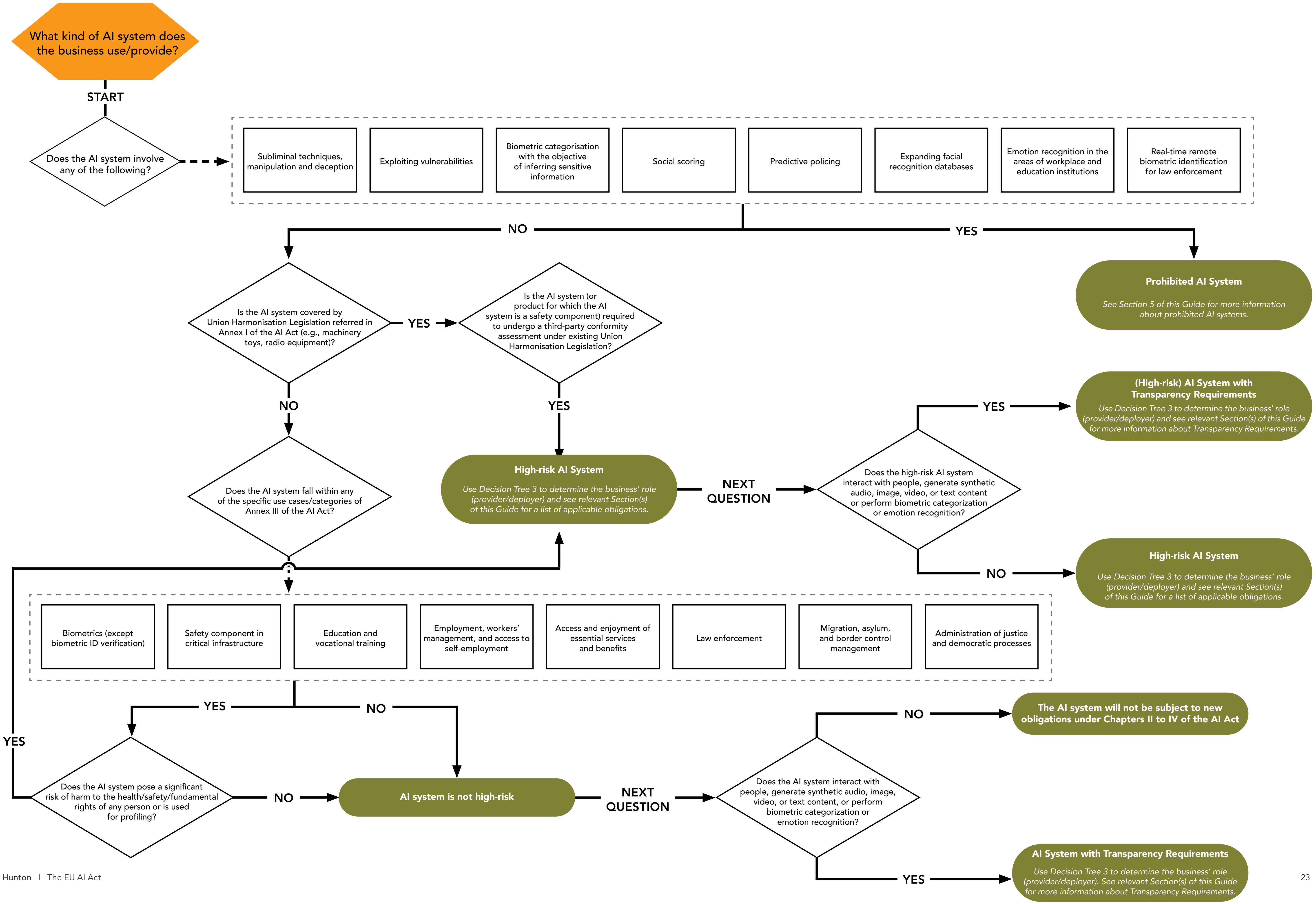
The business is providing a general-purpose AI model within the meaning of the AI Act

See Section 7 of the guide for more information about the obligations applicable to general-purpose AI models.

NO

The business is not providing a general-purpose AI model within the meaning of the AI Act

Decision Tree 2: Type of AI System



What kind of AI system does the business use/provide?

START

Does the AI system involve any of the following?

- Subliminal techniques, manipulation and deception
- Exploiting vulnerabilities
- Biometric categorisation with the objective of inferring sensitive information
- Social scoring
- Predictive policing
- Expanding facial recognition databases
- Emotion recognition in the areas of workplace and education institutions
- Real-time remote biometric identification for law enforcement

YES → **Prohibited AI System**

See Section 5 of this Guide for more information about prohibited AI systems.

NO → Is the AI system covered by Union Harmonisation Legislation referred in Annex I of the AI Act (e.g., machinery toys, radio equipment)?

YES → Is the AI system (or product for which the AI system is a safety component) required to undergo a third-party conformity assessment under existing Union Harmonisation Legislation?

YES → **High-risk AI System**

Use Decision Tree 3 to determine the business' role (provider/deployer) and see relevant Section(s) of this Guide for a list of applicable obligations.

NEXT QUESTION → Does the high-risk AI system interact with people, generate synthetic audio, image, video, or text content or perform biometric categorization or emotion recognition?

YES → **(High-risk) AI System with Transparency Requirements**

Use Decision Tree 3 to determine the business' role (provider/deployer) and see relevant Section(s) of this Guide for more information about Transparency Requirements.

NO → **High-risk AI System**

Use Decision Tree 3 to determine the business' role (provider/deployer) and see relevant Section(s) of this Guide for a list of applicable obligations.

NO → Does the AI system fall within any of the specific use cases/categories of Annex III of the AI Act?

- Biometrics (except biometric ID verification)
- Safety component in critical infrastructure
- Education and vocational training
- Employment, workers' management, and access to self-employment
- Access and enjoyment of essential services and benefits
- Law enforcement
- Migration, asylum, and border control management
- Administration of justice and democratic processes

YES → Does the AI system pose a significant risk of harm to the health/safety/fundamental rights of any person or is used for profiling?

YES → High-risk AI System

NO → **AI system is not high-risk**

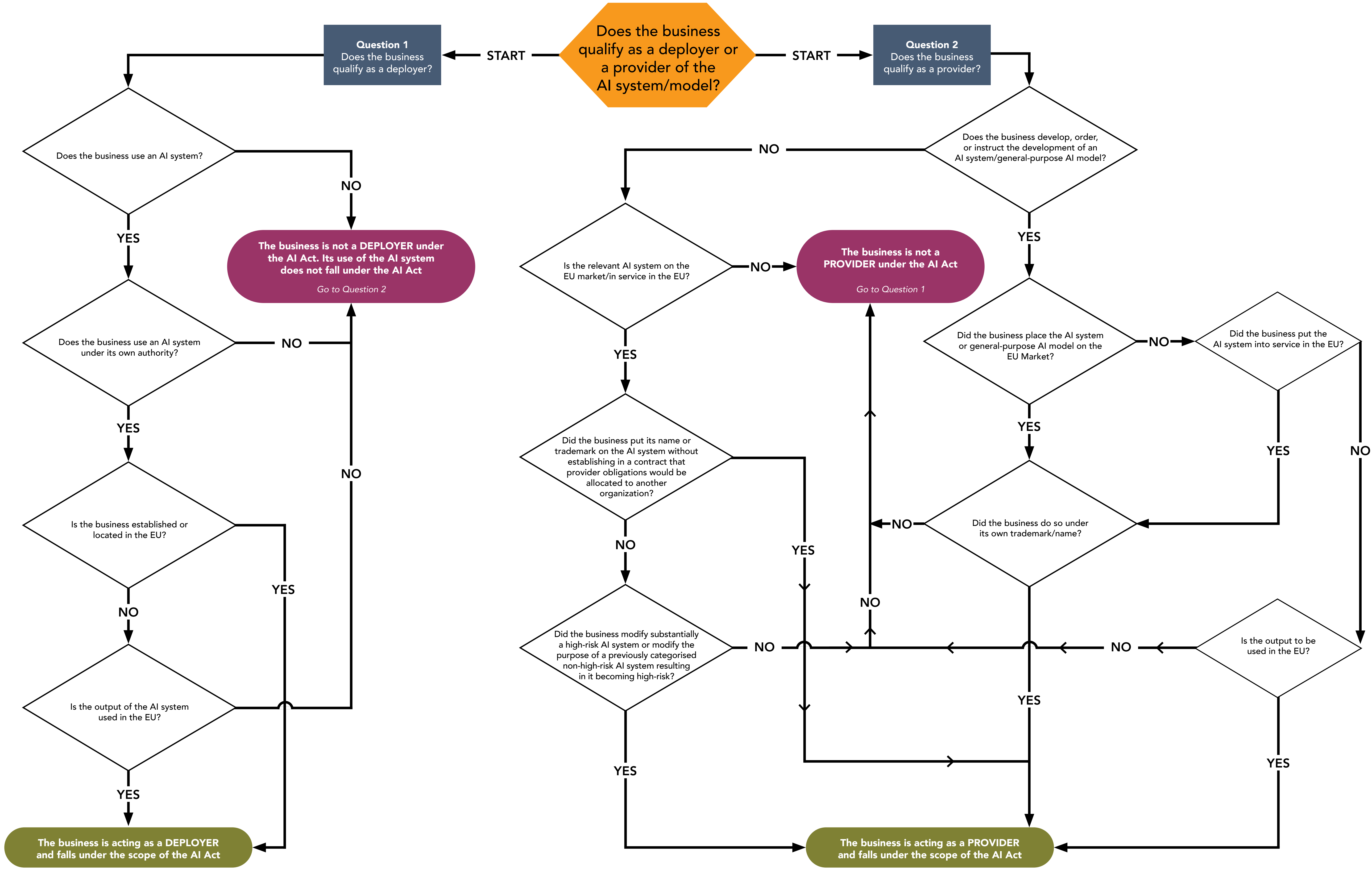
NEXT QUESTION → Does the AI system interact with people, generate synthetic audio, image, video, or text content, or perform biometric categorization or emotion recognition?

NO → **The AI system will not be subject to new obligations under Chapters II to IV of the AI Act**

YES → **AI System with Transparency Requirements**

Use Decision Tree 3 to determine the business' role (provider/deployer). See relevant Section(s) of this Guide for more information about Transparency Requirements.

Decision Tree 3: AI System Deployer or Provider



Does the business qualify as a deployer or a provider of the AI system/model?

Question 1
Does the business qualify as a deployer?

Does the business use an AI system?

Does the business use an AI system under its own authority?

Is the business established or located in the EU?

Is the output of the AI system used in the EU?

The business is not a DEPLOYER under the AI Act. Its use of the AI system does not fall under the AI Act

Go to Question 2

The business is acting as a DEPLOYER and falls under the scope of the AI Act

Question 2
Does the business qualify as a provider?

Does the business develop, order, or instruct the development of an AI system/general-purpose AI model?

Is the relevant AI system on the EU market/in service in the EU?

Did the business put its name or trademark on the AI system without establishing in a contract that provider obligations would be allocated to another organization?

Did the business modify substantially a high-risk AI system or modify the purpose of a previously categorised non-high-risk AI system resulting in it becoming high-risk?

Did the business place the AI system or general-purpose AI model on the EU Market?

Did the business put the AI system into service in the EU?

Did the business do so under its own trademark/name?

Is the output to be used in the EU?

The business is not a PROVIDER under the AI Act

Go to Question 1

The business is acting as a PROVIDER and falls under the scope of the AI Act

6. Practical Obligations for All Businesses

AI Literacy

Type of businesses affected?

Providers and deployers (see Decision Tree 3 in Section 5 of this Guide).

Type of systems affected?

All AI systems and AI models under the scope of the AI Act (see Decision Tree 1 in Section 5 of this Guide).

AI Literacy
(Article 4)

REQUIREMENTS

Both providers and deployers are required to take measures to ensure a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education, and training, the context the AI systems are to be used in, and the persons or groups of persons on whom the AI systems are to be used. This obligation is applicable to all types of AI systems and models under the scope of the AI Act.

PRACTICAL COMPLIANCE STEPS

Businesses should evaluate the AI systems that they are providing or deploying and ensure that their staff are adequately prepared to work with these systems in a manner that protects the fundamental rights of individuals. A robust AI training programme, which is kept up to date, will be essential to comply with this provision.

INTERPLAY WITH THE GDPR

Under the accountability principle, businesses are required to have in place measures to ensure that their staff and other persons under their responsibility receive training with regards to the protection of personal data. Businesses will likely be able to leverage current GDPR education and training programmess to develop AI literacy measures under the AI Act.

7. Practical Obligations for Businesses: Provider Obligations

High-risk AI Systems

Type of businesses affected?

Providers (see Decision Tree 3 in Section 5 of this Guide).

Type of systems affected?

High-risk AI systems (see Decision Tree 2 in Section 5 of this Guide).

Risk Management System

(Article 9)

REQUIREMENTS

Providers are required to establish, implement, document, and maintain a risk management system for high-risk AI systems, throughout the entire lifecycle of the AI system.

The risk management system shall consist of the following steps:

a. identification and analysis of the reasonably foreseeable risks that the system may pose to health, safety, or fundamental rights when used in accordance with its intended purpose;

b. estimation and evaluation of the risks that may emerge when the system is used for its intended purpose and under conditions of reasonably foreseeable misuse;

c. evaluation of risks based on the analysis of data gathered from the post-market monitoring system; and

d. adoption of appropriate and targeted risk management measures designed to address the risks identified through the above steps.

The risks identified through the risk management system must be at a level that the residual risk associated with each hazard, as well as the overall residual risks of the high-risk AI system, are acceptable. Where appropriate, adequate mitigation, and control measures should be adopted for risks that cannot be eliminated.

High-risk AI systems must be tested to identify the most appropriate and targeted risk management measures in order to ensure the systems perform consistently for their intended purpose. The risk management system must also take into consideration whether the high-risk AI system is likely to be accessed by or have an impact on persons under the age of 18 or other vulnerable groups.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems will need to develop and implement a risk management system that meets the minimum requirements identified in the AI Act. In practice, this will require providers to implement internal policies, procedures and processes that enable them to:

a. Identify, analyse, and evaluate reasonably foreseeable risks, including those that arise from potential misuse of the system;

b. Establish a post-market monitoring system; and

c. Implement measures to mitigate any identified risks.

These risk management measures must be applied from the initial development phase and throughout the entire lifecycle of any high-risk AI system. Providers should document and be prepared to explain their choices as regards the implementation of risk management measures. This may require the involvement of experts and external stakeholders.

INTERPLAY WITH THE GDPR

Pursuant to Article 24(1) of the GDPR, businesses are required to implement appropriate accountability measures to be able to demonstrate that processing is performed in accordance with the GDPR. When doing so, businesses must take into consideration the risks such processing poses to individuals. In addition, Article 25(1) of the GDPR requires businesses to integrate data protection into their processing activities and business practices, from the design phase through the lifecycle of a product. This is known as "data protection by design and by default". It requires businesses to consider at the initial phase of any system, service, product, or process, the risk that it may pose to individuals. Further, Article 35(1) of the GDPR requires businesses to perform DPIAs to help them identify and minimise the data protection risks of a project. A DPIA must identify and assess risks to individuals and any additional measures to mitigate those risks. Article 9 of the AI Act creates risk management requirements of a similar nature to those under the GDPR, albeit broader in scope, for high-risk AI systems.

Measures implemented to comply with the risk assessment and management requirements under the GDPR may be leveraged as relevant components of the risk management system required under the AI Act. Providers acting as controllers under the GDPR will already be familiar with the GDPR obligation to perform DPIAs and other information risk assessments under the GDPR (e.g., when considering security measures).

Data Quality, Data Governance and Management

(Article 10)

REQUIREMENTS

High-risk AI systems that use techniques involving the training of AI models with data must be developed using training, validation and testing data sets that are subject to appropriate governance and management practices. These data governance and management practices must be appropriate for the intended purpose of the relevant high-risk AI system and concern in particular:

a. Design choices;

b. Data collection processes, the origin of data, and in the case of personal data, the original purpose of the data collection;

c. Data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;

d. The formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent;

e. An assessment of the availability, quantity, and suitability of the data sets that are needed;

f. An examination of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under EU law, especially where data outputs influence inputs for future operations;

g. Appropriate measures to detect, prevent, and mitigate possible biases identified above; and

h. The identification of relevant data gaps or shortcomings that prevent compliance with the AI Act, and measures to address those gaps and shortcomings.

In addition, the training, validation, and testing data sets must fulfil certain quality criteria, particularly:

a. Be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose;

b. Have the appropriate statistical properties, including regarding the persons in relation to whom the high-risk AI system is intended to be used; and

c. Take into account the geographical, contextual, behavioural, or functional setting within which the high-risk AI system is intended to be used.

Training, validation, and testing data sets may only include special categories of personal data (as defined under the GDPR) in exceptional circumstances, when the processing of such data is strictly necessary for bias detection and correction, and appropriate safeguards are in place, including:

a. The bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data;

b. The data are subject to limitations of re-use, and privacy-preserving measures are taken, including pseudonymisation;

c. The data are kept secured and are subject to strict access controls and logs, to ensure that only authorised persons with confidentiality obligations have access to the personal data;

d. The data are not transmitted or otherwise accessed by other parties;

e. The data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first; and

f. The GDPR records of data processing activities include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct bias, and why that objective could not be achieved by processing other data.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems that train their AI models with data must implement internal data quality processes and controls for training, validation, and testing data. Developing systems, checklists, and standard operation procedures, and appropriately allocating available resources and creating an oversight mechanism will be helpful in ensuring and monitoring compliance with this requirement on an ongoing basis.

The measures that providers must implement to address these data quality and data governance obligations should also be aligned with their obligations for a quality management system under Article 17 of the AI Act (see page 34 of this Guide).

INTERPLAY WITH THE GDPR

The data quality requirements under the AI Act partially overlap with the general principles of the GDPR, including the accountability and accuracy requirements. That said, the data quality requirements under the AI Act are more specific, and technical, and also apply to non-personal data. Existing internal policies and procedures drafted for GDPR compliance purposes can be leveraged but likely will require updates or new processes (some technical) to ensure compliance with the AI Act's specific data quality criteria for training, validation and testing data in connection with the development of high-risk AI systems.

Regarding the use of special categories of personal data for training of AI models, there is significant overlap between the specific conditions that apply in connection with including special categories of personal data in the training, validation, and testing data under the AI Act, and the obligation to carry out a DPIA under the GDPR. In practice, businesses likely will be able to leverage existing processes and assessments to address both requirements simultaneously. In addition, the AI Act includes express reference to updating records of processing activities under the GDPR to include specific content.

Technical Documentation of High-risk AI Systems

(Article 11)

REQUIREMENTS

Before placing on the market or putting into service a high-risk AI system, providers are required to draw up the technical documentation with respect to the system. The technical documentation must be clear and comprehensive and be kept up to date for the lifetime of the system. At a minimum, and as applicable to the relevant AI system, the technical documentation must contain the following elements (Annex IV of the AI Act):

1. **A general description of the AI system including:**
   a. Its intended purpose, the name of the provider, and the version of the system reflecting its relation to previous versions;
   b. How the AI system interacts with hardware/software, including other AI systems;
   c. The versions and version updates of relevant software or firmware;
   d. The description of all the forms in which the AI system is placed on the market or put into service, such as software packages embedded into hardware, downloads, or APIs;
   e. The description of the hardware on which the AI system is intended to run;
   f. Where the AI system is a component of products, photographs, or illustrations showing external features, the marking, and internal layout of those products;
   g. A basic description of the user-interface provided to the deployer; and
   h. Instructions for use for the deployer and a basic description of the user-interface provided to the deployer.
2. **A detailed description of the elements of the AI system and of the process for its development, including:**
   a. The methods used and steps performed for the development of the AI system;
   b. The design specifications of the AI system, namely the general logic of the AI system and of the algorithms; the key design choices including the rationale and assumptions made, including with regard to persons or groups of persons in respect of whom the system is intended to be used; the main classification choices; what the system is designed to optimise, and the relevance of the different parameters; the description of the expected output and output quality of the system; and decisions made about any possible trade-offs regarding the technical solutions adopted to comply with the requirements under the AI Act;
   c. The description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing; the computational resources used to develop, train, test, and validate the AI system;
   d. Where relevant, the training methodologies and the training data sets used, how the data was obtained and selected, labelling procedures, and data cleaning methodologies;
   e. An assessment of the human oversight measures needed;
   f. Where applicable, a detailed description of pre-determined changes to the AI system and its performance, together with all relevant information related to the technical solutions adopted to ensure continuous compliance of the AI system with relevant requirements;
   g. The validation and testing procedures used, including information about the validation and testing data used and their main characteristics; metrics used to measure accuracy, robustness, and potentially discriminatory impacts; test logs and all test reports dated and signed by the responsible persons, including with regard to pre-determined changes; and
   h. Cybersecurity measures put in place.
3. **Detailed information about the monitoring, functioning, and control of the AI system, in particular with regard to its capabilities and limitations in performance (i.e., degrees of accuracy, overall expected level of accuracy, foreseeable unintended outcomes and sources of risks, human oversight measures needed, specifications on input data);**
4. **A description of the appropriateness of the performance metrics for the specific AI system;**
5. **A detailed description of the risk management system under Article 9 of the AI Act;**
6. **A description of relevant changes made by the provider to the system through its lifecycle;**
7. **A list of the EU harmonised standards or other relevant standards and technical specifications applied;**
8. **A copy of the EU declaration of conformity; and**

9. **A detailed description of the system in place to evaluate the AI system performance in the post-market phase (post-market monitoring plan).**

Depending on the provider's sector, there could be areas of overlap with other EU legislation that also require preparation and maintenance of technical documentation. In that case, producing a single set of technical documentation will be permitted as an exception.

SMEs and start-ups may provide the elements of the technical documentation specified in Annex IV of the AI Act in a simplified manner. The EU Commission is required to develop a simplified form for those entities.

PRACTICAL COMPLIANCE STEPS

Providers will need to prepare new technical documentation that meets the specific content requirements before placing on the market or putting into service a high-risk AI system. In addition, internal policies and procedures will need to be implemented to ensure that the technical documentation is updated throughout the AI system's lifetime. The technical documentation will be an important accountability tool, as the documentation is intended to ensure the traceability of the system, verify compliance with the requirements of the AI Act, and document the post-market monitoring measures implemented by the provider.

Given the level of technical details required for compliance with this obligation, providers may consider involving a multidisciplinary team composed of various internal stakeholders (e.g., such as the engineering, legal, operations, and business teams) to develop, monitor, and keep up-to-date the technical documentation required for high-risk AI systems.

INTERPLAY WITH THE GDPR

The requirement for technical documentation of high-risk AI systems is new and does not have an overlap with an existing obligation under the GDPR. Businesses will need to develop new compliance documentation and processes to comply with this new requirement under the AI Act, unless an exception applies. That said, businesses may be able to leverage certain GDPR accountability efforts in the process of preparing technical documentation, such as for the description of the applicable cybersecurity measures.

Record-keeping Obligations
(Articles 12 and 19)

REQUIREMENTS

High-risk AI systems must technically allow for the automatic recording of events ("logs") over the lifetime of the system.

Logging capabilities must enable the recording of events relevant for:

a. Identifying situations that may result in a risk or in a substantial modification;

b. Facilitating post-market monitoring; and

c. Monitoring the operation of high-risk AI systems.

Under Article 19 of the AI Act, logs that are under the provider's control should be retained for a period that is appropriate considering the intended purpose of the AI system. This period should be, at least, six months.

For remote biometric identification systems, the logging capabilities must capture, at a minimum:

a. A record of the period (start date/time, end date/time) of each 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 identification of the individuals involved in the verification of the results (i.e., human oversight/verification by at least two persons separately).

PRACTICAL COMPLIANCE STEPS

The logs required under the AI Act likely will require configuring the systems with specific settings and parameters. In addition, the development of checklists and monitoring processes will be helpful, as this is a requirement that applies "over the lifetime" of high-risk AI systems.

INTERPLAY WITH THE GDPR

⊖ The logging requirements partially overlap with the data security requirements and best practices under the GDPR, but are more specific and require technical implementation. It is expected that providers will develop and implement technical capabilities and specific processes to comply with this requirement. Providers will also be required to consider the retention period for logs in their data protection retention schedules.

Transparency and Provision of Information from Providers to Deployers (Article 13)

REQUIREMENTS

The providers of high-risk AI systems must ensure that the operation of the AI system is sufficiently transparent to deployers so they can interpret the system's output appropriately.

High-risk AI systems must be accompanied by instructions for use addressed to deployers that are concise, complete, correct, clear, relevant, accessible, and comprehensible. The instructions for use must include:

1. **The identity and contact details of the provider and, where applicable, its authorised representative;**
2. **The characteristics, capabilities, and limitations of the high-risk AI system, including:**
   a. Its intended purpose;
   b. The level of accuracy (incl. metrics), robustness and cybersecurity; and
   c. Any known or foreseeable circumstance, or reasonably foreseeable misuse, which may lead to risks to the health and safety of individuals or their fundamental rights;

   and where applicable or appropriate:

   a. Information that is relevant to explain the output of the high-risk AI system;
   b. The performance of the high-risk AI system regarding specific persons on which it is intended to be used;
   c. Specifications for the input data (including training, validation, and testing data sets used); and
   d. Information to enable deployers to interpret the output of the high-risk AI system and use it appropriately;
3. **The changes to the high-risk AI system which have been predetermined by the provider;**
4. **Human oversight measures, including the technical measures put in place to facilitate the interpretation of the outputs of the high-risk AI systems by the deployers;**
5. **The computational and hardware resources needed, the AI system's expected lifetime, any necessary maintenance and its frequency (including software updates); and**
6. **The mechanisms that allow deployers to collect, store and interpret logs (where relevant).**

PRACTICAL COMPLIANCE STEPS

Providers need to ensure that the operation of their AI systems is sufficiently transparent and can be understood and used adequately by deployers. This may require adding capabilities to systems and configuring them with specific settings and parameters. Providers are also required to draft instructions for use addressed to deployers that cover certain minimum content requirements. That content is both legal and technical in nature. The instructions provided by providers are also intended to assist deployers in complying with their own obligations under the AI Act. See Section 8 of this Guide. In practice, providers likely will need to engage multidisciplinary teams to draft, review, and maintain those instructions of high-risk AI systems on an ongoing basis.

INTERPLAY WITH THE GDPR

There will be overlap with information provided in privacy notices under the GDPR, but the transparency requirements under Article 13 of the AI Act are detailed and technical in nature as opposed to principle-based. In addition, the transparency disclosures under Article 13 of the AI Act are addressed to deployers (which includes businesses), while the transparency disclosures under Article 13 and 14 of the GDPR are addressed to individuals. The transparency documentation under the GDPR can be used as a starting point as to how information is provided, however, additional efforts will be needed to provide the detailed information required under the AI Act in a clear and comprehensible manner. Where a deployer is a controller and the provider is a processor, the information received from the provider will be an important tool to evaluate whether the processor offers sufficient data protection guarantees and safeguards.

Obligations Related to Human Oversight
(Article 14)

REQUIREMENTS

Providers are required to design and develop AI systems in a way that ensures effective oversight by natural persons. Oversight measures should aim at preventing or minimizing the risks to health, safety, or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. The measures must be tailored to the risks, level of autonomy, and context of use of the AI system and should include one or more of the following types of measures:

- Measures identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service; and
- Measures identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user.

The measures implemented in light of the oversight requirement should enable the person responsible to oversee the system to:

- Properly understand its capacities and limitations and be able to monitor the system;
- Remain aware of automation bias;
- Interpret the output of the AI system; and
- Decide whether to use the AI system or disregard, override, or reverse its input and to intervene in the operation of the AI system or interrupt it (e.g., through a "stop button").

Additional human oversight requirements will also apply to remote biometric identification systems referred to in point 1(a) of Annex III.

PRACTICAL COMPLIANCE STEPS

Providers will need to assess the necessary measures to guarantee effective human oversight taking into account the expected risks and context of use of their AI systems, along with their level of autonomy. Depending on the specific context, such measures may either be built into the system itself and/or be made available to deployers for implementation.

When selecting which types of measures to implement, providers should ensure that they provide the necessary conditions for the human oversight to be efficient, as required by the AI Act (e.g., allow the human overseer to remain aware of automation bias). This may include ensuring that the output of the AI system is understandable by a human overseer, making available a description of the capabilities and limitations of the AI system to the overseer and/or making available technical solutions allowing the overseer to disregard, override, or reverse the input of the AI systems, intervene in its operation or interrupt it.

INTERPLAY WITH THE GDPR

Pursuant to Article 22(1) of the GDPR, individuals have the right not to be subject to a decision based solely on automated processing which produces legal or similarly significant effects for these individuals, except in specific situations, such as if they have explicitly consented to it. Article 22(3) of the GDPR requires controllers to implement measures to safeguard individuals' rights and freedoms and legitimate interests, including to obtain human intervention, express their point of view, and contest the decision. Article 14 of the AI Act creates a similar human oversight requirement for high-risk AI systems.

The measures implemented to comply with the human oversight obligation applicable to automated individual decision-making under the GDPR may be leveraged by providers to comply with the rules applicable under Article 14 of the AI Act. In particular, providers acting as controllers under the GDPR will already be familiar with the GDPR obligation to ensure human oversight when taking automated-decisions. Providers acting as processors are also likely to implement measures ensuring human oversight in relation to their systems in order to assist their clients (i.e., the controllers) to comply with their own obligations. Controllers who qualify as deployers may consider requesting providers to clarify which measures their system implement to support human oversight.

Obligations Related to Accuracy, Robustness, and Cybersecurity
(Article 15)

REQUIREMENTS

Providers must design and develop high-risk AI systems in a way that ensures an appropriate level of accuracy, robustness, and cybersecurity throughout the lifecycle of the systems.

This entails that high-risk AI systems should be resilient against errors, faults, or inconsistencies. The relevant accuracy level and the accuracy metrics of high-risk AI systems must be specified in the instructions of use. High-risk AI systems should also be resistant to attempts to alter their use, outputs, or performance by exploiting the system vulnerabilities.

Additionally, for systems that continue to learn after they are placed on the market, providers must implement measures to eliminate or reduce feedback loops as much as possible.

PRACTICAL COMPLIANCE STEPS

Providers should integrate the security, robustness, and cybersecurity requirements of the AI Act into their development procedures. When relying on third parties for the development of high-risk AI systems, providers should ensure that these third-parties adequately consider these requirements. The measures implemented to address these issues should be documented and records must be kept available should they be requested by the MSA.

Note: Providers of high-risk AI systems that also fall under the scope of the EU's Cyber Resilience Act will be able to demonstrate compliance with the cybersecurity requirement of the AI Act by fulfilling the essential cybersecurity requirements set out in the Cyber Resilience Act. Considering the broad scope of application of the Cyber Resilience Act, AI system providers should carefully consider if their systems fall under the two sets of rules and leverage existing synergies. See Section 1 of this Guide.

INTERPLAY WITH THE GDPR

When high-risk AI systems are used to process personal data, Article 15 of the AI Act will need to be read in conjunction with the security and accuracy principles of the GDPR (Articles 5(1)(f) and (d) and Article 32 of the GDPR). While the measures required by the AI Act are more specific in nature, providers who already develop their AI systems considering the security and accuracy requirements of the GDPR will have a head start in complying with Article 15 of the AI Act.

Provision of Information to End-users
(Article 16(b))

REQUIREMENTS

Providers must indicate their name, registered trade name or registered trademark, and contact address on the high-risk AI system itself or, where that is not possible, on the system's packaging or accompanying documentation.

PRACTICAL COMPLIANCE STEPS

Providers will need to assess how to best provide the legally required information to end-users and ensure that their system, packaging, or documentation include the required content.

INTERPLAY WITH THE GDPR

Although both the AI Act and the GDPR impose transparency requirements *vis-à-vis* end-users, the information/transparency requirements under the AI Act are substantially different from the transparency requirements applicable under the GDPR (e.g., Articles 13 and 14) and GDPR compliance measures will generally not be suitable for compliance with this requirement under the AI Act.

Accessibility

(Article 16(l))

REQUIREMENTS

Providers of high-risk AI systems must ensure that their systems comply with accessibility requirements in accordance with the Accessibility Directives which impose rules for accessible products and services.

These requirements mandate that products and services, especially those related to information and communication technologies (e.g., digital content, websites, software, mobile applications, and other ICT products and services) must be designed and developed in a way that ensures accessibility for all users, including those with disabilities.

PRACTICAL COMPLIANCE STEPS

Providers will need to ensure that any high-risk AI systems meet applicable EU accessibility requirements. This includes considering:

a. whether the features or functionalities of the high-risk AI systems (e.g., instructions, support services, user interfaces) are sufficiently accessible for all users; and

b. whether any exemptions may apply under Accessibility Directives and if so, how to properly conduct and document that assessment.

INTERPLAY WITH THE GDPR

The GDPR does not impose similar accessibility requirements on businesses. As such, businesses will generally not be able to leverage their GDPR compliance measures to address this requirement under the AI Act. That said, under the GDPR, businesses are required to implement appropriate technical and organisational measures to ensure the security and protection of personal data, especially when processing data of vulnerable individuals, such as children or individuals with special needs. This involves taking extra precautions to safeguard the privacy and rights of these individuals, considering their increased vulnerability to potential risks associated with data processing. For example, additional transparency requirements apply when providing information on the processing of personal data to children. In addition, when processing data of vulnerable individuals, such as children or individuals with special needs or disabilities, there is an increased risk of harm or infringement of their rights due to their heightened vulnerability and such processing activities are therefore likely to trigger the requirement for a DPIA.

The Quality Management System

(Article 17)

REQUIREMENTS

Providers of high-risk AI systems are required to implement a quality management system ("QMS") that ensures compliance with the AI Act. The QMS needs to be documented by way of policies, procedures, and instructions.

The QMS must include the following (at a minimum):

a. A strategy for regulatory compliance, including procedures for managing modifications to the system;

b. Techniques, procedures, and systematic actions for the design, design control, and design verification of the system;

c. Techniques, procedures, and systematic actions for the development, quality control, and quality assurance of the system;

d. Examination, test, and validation procedures, and the frequency with which they have to be carried out;

e. Technical specifications and standards to be applied to the system;

f. Systems and procedures for data management;

g. The risk management system referred to in Article 9 of the AI Act;

h. The establishment, implementation, and maintenance of a post-market monitoring system to ensure the system remains compliant with the AI Act throughout its lifetime;

i. Procedures related to the reporting of a serious incident in accordance with Article 73 of the AI Act;

j. The handling of communication with national competent authorities, other relevant authorities, notified bodies, other operators, customers, or other interested parties;

k. Systems and procedures for record keeping of all relevant documentation and information;

l. Resource management, including security of supply related measures; and

m. An accountability framework setting out the responsibilities of the management and other staff with regard to all aspects of the QMS.

PRACTICAL COMPLIANCE STEPS

In practice, providers of high-risk AI systems will need to develop and implement a QMS consisting of written policies, procedures and instructions, including (i) detailed technical documentation about the relevant system; (ii) quality control and quality assurance procedures; (iii) systems and procedures for data management (covering data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention, and other data-related operations); and (iv) a post-market compliance monitoring system.

Providers of AI systems that are subject to the obligation to implement QMSs or equivalent functions under sectorial EU legislation (e.g., in the medical device, machinery, or radio equipment sector) may leverage their existing QMS for compliance with the AI Act by integrating applicable requirements for AI compliance.

INTERPLAY WITH THE GDPR

The GDPR imposes accountability obligations that require businesses to implement and maintain policies and procedures to demonstrate compliance with their obligations. While the QMS requirements in the AI Act are substantively different in nature to the requirements applicable under the GDPR, they share a similar accountability logic. Businesses may be able to leverage their current GDPR compliance measures and accountability framework, albeit with significant adaptations, to comply with certain QMS requirements (such as the implementation of systems and procedures for data management or the establishment of policies and procedures for communication with national competent authorities, other relevant authorities, notified bodies, other operators, customers, or other interested parties).

Documentation Keeping
(Article 18)

REQUIREMENTS

Providers of high-risk AI systems are required to store the following documents for a period of 10 years from the moment the system is placed on the market or put into service:

a. The technical documentation (see page 29 of this Guide);

b. The documentation concerning the quality management system (see page 34 of this Guide);

c. The documentation concerning the changes approved by notified bodies, where applicable (see page 39 of this Guide);

d. The decisions and other documents issued by the notified bodies, where applicable (see page 39 of this Guide); and

e. The EU declaration of conformity (see page 42 of this Guide).

These documents should be made available to the MSA or to the notifying authority on request.

Member States will establish additional rules to ensure that the documentation remains available if a provider or its authorised representative goes bankrupt or ceases their activity prior to the end of the mandatory storage period.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems should update their record retention policies and procedures to include the relevant business documents.

Considering that certain of the documents will contain personal data (e.g., signature, name, and function of the person responsible in the EU declaration of conformity or name and function of the person approving a procedure related to the quality management system), providers should also review and, if required, update their personal data retention schedules to account for the retention of this personal data.

INTERPLAY WITH THE GDPR

While these obligations apply to documentation related to AI Act requirements, providers may leverage their current record retention policies and procedures as above to include the relevant business documents. This includes the procedures addressing documentation required by the GDPR which is subject to significant retention periods in order to prove compliance with applicable legal obligations at the request of a DPA or a court (e.g., records of processing activities, DPIAs, and legitimate interests assessments). With regard to personal data, providers may also be able to leverage their existing data retention schedules.

Corrective Actions

(Article 20)

REQUIREMENTS

Providers of high-risk AI systems are required to take corrective actions when they consider, or have reason to consider, that an AI system is not in compliance with the AI Act. Such actions may include withdrawing, disabling, or recalling the AI system.

Providers must inform deployers, distributors, importers, and authorised representatives of the corrective actions implemented.

As per Article 3(19) of the Market Surveillance Regulation, providers must immediately investigate if they become aware that their high-risk AI system has potential to adversely affect: (i) health and safety of persons in general; (ii) health and safety in the workplace; (iii) protection of consumers; (iv) the environment; (v) public security; (vi) other public interests, to a degree which goes beyond that considered reasonable and acceptable in relation to the AI system's intended purpose or under the normal or reasonably foreseeable conditions of its use. In this case, providers should notify the MSA and, when applicable, the notified body which issued the certificate for the AI system.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems will need to maintain oversight over their AI systems even after they have been placed on the market or put into service to ensure that they detect any changes in their state of compliance and take measures promptly.

The post-market monitoring system, to be put in place under Article 72 of the AI Act (see page 45 of this Guide on the post-market monitoring system), will be a key piece in ensuring compliance with the rules under Article 20 of the AI Act.

Additionally, providers should maintain lines of communication with other businesses in the AI value chain, such as deployers, to ensure that they are able to communicate any corrective actions taken. Providers should establish clearly in their agreements with these businesses how they will inform them when required.

Lastly, providers should establish internal procedures to ensure that they are able to identify cases where there is a significant increase in the risk of the AI systems which may require notification to the MSA and notified bodies.

INTERPLAY WITH THE GDPR

Under the GDPR, controllers must also deploy corrective steps in case they detect that a processing operation for which they are responsible is no longer in compliance with the law. This may require changes to how certain products work. The logic behind the GDPR's rule and Article 20 of the AI Act is similar, and businesses may be able to leverage continuous privacy risk assessment processes that have been implemented from a privacy-by-design perspective for their compliance with the AI Act.

However, the product safety structure of the AI Act, along with the interplay of Article 20 with other provisions of the AI Act such as Article 72, and the requirement to potentially engage with a great number of stakeholders such as the MSA or deployers, makes the obligation under the AI Act more complex than the GDPR requirement.

Cooperation with Competent Authorities
(Article 21)

REQUIREMENTS

Upon a reasoned request by a competent authority, providers of high-risk AI systems must provide that authority with all information and documentation necessary to demonstrate conformity with the requirements for high-risk AI systems. This information must be provided in a language which can be easily understood by the authority.

This also includes giving the requesting authority access to the automatically generated event logs of the high-risk AI system, to the extent such logs are under a provider's control.

Any information obtained by a competent authority pursuant to Article 21 shall be treated confidentially in accordance with the confidentiality obligations set out in Article 78.

The cooperation obligations established in Article 21 are without prejudice to the extensive powers on market surveillance, investigation, and enforcement provided to the MSAs through the Market Surveillance Regulation (see Section 9 of this Guide on Supervision and Enforcement).

PRACTICAL COMPLIANCE STEPS

To assist in complying with such cooperation obligations, providers should consider:

a. Establishing internal policies and procedures for responding to requests and inquiries from competent authorities;

b. Designating a point of contact with responsibility for liaising with competent authorities;

c. Training relevant personnel on their obligations and procedures for cooperation with competent authorities; and

d. Maintaining comprehensive documentation related to their AI systems and ensuring such documentation is appropriately filed and available upon request.

INTERPLAY WITH THE GDPR

Article 31 of the GDPR requires both controllers and processors to cooperate, on request, with DPAs in the performance of their tasks. This obligation extends to the provision of information necessary to demonstrate compliance with the GDPR and cooperation with investigations conducted by a DPA which is similar to the cooperation obligations established in the AI Act.

While requests for cooperation made under the GDPR and AI Act are likely to be different in practice, businesses will be able to leverage any GDPR cooperation procedures and mechanisms for the purpose of complying with the cooperation obligations under the AI Act. This will be particularly helpful in countries where the DPA is also appointed as the MSA under the AI Act.

Authorised Representatives of Providers of High-risk AI Systems
(Article 22)

REQUIREMENTS

Before making a high-risk AI system available on the EU market, providers established outside the EU will have to appoint a representative established in the EU through a written mandate.

The mandate should enable the representative, at a minimum, to:

a. Verify that the EU declaration of conformity (Article 47 of the AI Act) and the technical documentation (Article 11 of the AI Act) have been drawn up and that an appropriate conformity assessment procedure has been carried out by the provider;

b. Keep at the disposal of the competent authorities and national authorities or bodies, for a period of 10 years after the high-risk AI system has been placed on the market or put into service, the contact details of the provider that appointed the authorised representative, a copy of the EU declaration of conformity, the technical documentation, and, if applicable, the certificate issued by the notified body;

c. Upon a reasoned request, provide a competent authority with all information and documentation necessary to demonstrate the conformity of a high-risk AI system with the requirements applicable to this type of system under the AI Act, including access to the logs automatically generated by the high-risk AI system (to the extent such logs are under the control of the provider);

d. Upon a reasoned request, cooperate with a competent authority in any action one may take in relation to the high-risk AI system, in particular to reduce and mitigate the risks posed by the high-risk AI system; and

e. Where applicable, comply with the registration obligations referred to in Article 49(1) of the AI Act, or, if registration is carried out by the provider itself, ensure that the information referred to in point 3 of Section A of Annex VIII is correct.

The mandate should also enable the authorised representative to be addressed, in addition to or instead of the provider, by competent authorities, on all issues related to the compliance with the AI Act.

At the request of the MSA, the authorised representative must provide a copy of the mandate in one of the official languages of the EU's institutions.

The authorised representative is required to terminate the mandate if it considers that the provider is acting contrary to its obligations under the AI Act and to inform the MSA and, where applicable, the relevant notified body, of the termination and reasons for doing so.

PRACTICAL COMPLIANCE STEPS

Businesses established outside the EU that intend to make high-risk AI systems available on the EU market should establish a relationship with an EU representative.

It is important that providers carefully select their representatives, verify their technical capabilities and establish a relationship of trust to ensure that both are able to act in a coordinated manner.

INTERPLAY WITH THE GDPR

Similar to Article 22 of the AI Act, Article 27 of the GDPR requires certain businesses established outside the EU but subject to the extraterritorial application of the GDPR to appoint an EU representative. While the specific tasks of the representative are different under the AI Act and the GDPR, the logic behind both provisions is the same: having a point of contact in the EU capable of carrying out certain obligations and engaging with competent authorities. Businesses may even be able to appoint their current GDPR representatives as representatives under the AI Act if they have the technical capability to carry out the additional tasks established in the AI Act.

Harmonised Standards, Standardisation Deliverables, and Common Specifications

(Articles 40 and 41)

REQUIREMENTS

Harmonised Standards and Standardisation Deliverables

High-risk AI systems that are in conformity with harmonised standards related to certain goods and services in accordance with the Standardisation Regulation are presumed to be in conformity with the requirements for high-risk AI systems under the AI Act (as set out in Section 2 of Chapter III of the AI Act or, as applicable, the obligations set out in Chapter V of AI Act). The EU Commission is required to issue standardisation requests covering relevant AI Act requirements to standardisation organisations.

Common Specifications

The EU Commission is empowered to adopt implementing acts establishing common specifications for the requirements for high-risk AI systems (as set out in Section 2 Chapter III of the AI Act or, as applicable, the obligations set out in Chapter IV of AI Act).

High-risk AI systems adhering to common specifications adopted by the EU Commission will be assumed to meet the requirements for high-risk AI systems, as long as those specifications address the requirements. Providers of high-risk AI systems not complying with these common specifications will need to explain how they have implemented alternative technical solutions to meet the same requirements.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems should assess whether their systems conform with existing harmonised standards after they are issued or common specifications approved by the EU Commission as a means of demonstrating compliance with the requirements for high-risk AI systems under the AI Act. This assessment should be documented internally. Providers should also continue to monitor the development of relevant harmonised standards and common specifications as these may facilitate their compliance efforts.

INTERPLAY WITH THE GDPR

Article 40 of the GDPR encourages the drawing up of codes of conduct that controllers and processors can certify to in order to demonstrate compliance with their obligations under the GDPR. In addition, Article 42 of the GDPR encourages the use of certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR.

The codes of conduct and certification mechanisms contemplated by the GDPR serve a similar purpose to the harmonised standards or common specifications but the application of these concepts is likely to be different. In particular, GDPR codes of conduct and certifications are likely to apply only to GDPR compliance issues. As a result, businesses will generally not be able to leverage existing GDPR codes of conduct or certification schemes for the purpose of demonstrating conformity with harmonised standards or common specifications under the AI Act.

Conformity Assessment Procedure
(Article 43)

REQUIREMENTS

Conformity assessment procedures aim at demonstrating whether the requirements under the AI Act for high-risk AI systems have been satisfied. Providers of high-risk AI systems are required to ensure that their systems undergo a conformity assessment procedure. The type of assessment and rules applicable to the conformity assessment procedure will vary depending on the specific systems.

- **General framework applicable to high-risk AI systems:** Providers of high-risk AI systems listed in points 2 to 8 of Annex III must follow the conformity assessment procedure described in Annex VI which is simplified and based on internal control.
- **Biometric AI systems:** With respect to biometric high-risk AI systems (listed in point 1 of Annex III of the AI Act), where the provider has demonstrated compliance with the requirements for high-risk AI systems using the harmonised standards (Article 40 of the AI Act) or common specifications (Article 41 of the AI Act), the provider must choose one of the following conformity assessment procedures based on:

a. internal control (Annex VI of the AI Act); or

b. involvement of a notified body (Annex VII of the AI Act).

In demonstrating compliance with the requirements for biometric high-risk AI systems, the provider will be required to follow the conformity assessment procedure set out in Annex VII of the AI Act where:

a. harmonised standards do not exist, and common specifications are not available;

b. the provider has not applied the harmonised standard in full;

c. common specifications exist but have not been applied; or

d. one or more of the harmonised standards referred to in point (a) has been published with a restriction, and only on the part of the standard that was restricted.

The conformity assessment procedure under Annex VII of the AI Act is more comprehensive and requires the evaluation of the quality management system and technical documentation by a third-party (i.e., the notified body). For the purposes of this conformity assessment procedure, the provider may choose any of the notified bodies, except where the high-risk AI system will be used by law enforcement, immigration or asylum authorities or by EU institutions, bodies, offices or agencies, in which case the MSA shall act as a notified body.

- **AI systems covered by Union harmonisation legislation:** AI systems that are considered high-risk because they are covered by Union harmonisation legislation and are listed in Section A of Annex I of the AI Act are subject to the third-party conformity assessment procedure established under the relevant harmonisation legislation. The AI Act's requirements for high-risk AI systems are also part of the assessment and selected rules of Annex VII will also apply. Notified bodies under the applicable Union harmonisation legislation will be able to control the conformity of high-risk AI systems as long as these notified bodies are in compliance with the requirements regarding independence, integrity, competence, and resources established under Article 31 (4), (5), (10) and (11) of the AI Act.
- **Additional requirements:** A new conformity assessment procedure must be undertaken in the event of a substantial modification to the relevant AI system, regardless of whether it has already been subject to a conformity assessment procedure.

With respect to high-risk AI systems that continue to learn after being placed on the market or put into service, it is important to note that changes to the performance of that system, which have been predetermined by the provider at the point of the initial conformity assessment and are part of the information contained in the technical documentation, will not constitute a substantial modification that would require a new conformity assessment procedure.

PRACTICAL COMPLIANCE STEPS

As a first step, providers of high-risk AI systems will need to identify which conformity assessment procedure applies to their system and ensure that the relevant procedure is followed.

For AI systems subject to the conformity assessment procedure based on internal control, providers should put in place the technical and organisational measures required to ensure that they are successfully capable of carrying out this procedure internally. Importantly, note that the MSA may request evidence that the conformity assessment procedure was properly carried out.

For AI systems subject to a third-party conformity assessment procedure, providers will need to identify an accredited conformity assessment body (notified body), provide the information and documentation required by Annex VII of the AI Act and cooperate with the notified body.

INTERPLAY WITH THE GDPR

The GDPR does not impose conformity assessment procedures on businesses. This type of procedure is more common in product safety legislation. As such, businesses will not be able to leverage their GDPR compliance measures to address this requirement under the AI Act.

That said, the GDPR requires controllers to conduct a DPIA when a processing activity is deemed likely to result in a high risk to the rights and freedoms of individuals. Hence, providers of high-risk AI systems that involve the processing of personal data will need to go through a conformity assessment procedure and conduct a DPIA. Conformity assessment procedures under the AI Act and DPIAs under the GDPR serve distinct purposes: a conformity assessment aims at ensuring compliance with specific legal requirements which aim at mitigating the risks related to high-risk AI systems, while a DPIA serves more as a tool for accountability and aims at assessing risks related to personal data processing. Businesses will likely not be able to leverage their DPIAs to address this requirement under the AI Act. However in practice, these two requirements will likely be connected for high-risk AI systems that involve the processing of personal data and there might be some interplay between certain elements to be evaluated under the conformity assessment procedure such as the technical documentation (Article 11 of the AI Act), the DPIA, and other compliance measures under the GDPR.

Conformity Assessment Procedure Based on Internal Control

(Annex VI)

REQUIREMENTS

The conformity assessment procedure based on internal control requires providers to:

a. Verify that the established quality management system complies with the AI Act's quality management system requirements, as set out in Article 17;

b. Examine the technical documentation in order to assess whether the AI system complies with the AI Act's requirements for high-risk AI systems, as set out in Title III, Chapter 2 of the AI Act; and

c. Verify that the AI system's design and development process and its post-market monitoring is consistent with the technical documentation.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems will need to establish processes and procedures to ensure that the AI system's established quality management system meets the requirements established under the AI Act.

In addition, providers will need to examine the AI system's technical documentation to ensure the system was developed and operates in accordance with such technical documentation, and meets the requirements applicable to high-risk AI systems.

INTERPLAY WITH THE GDPR

The GDPR does not include a conformity assessment procedure that businesses must follow. As such, businesses will not be able to leverage their GDPR compliance measures to address this requirement under the AI Act. However, there might be some interplay between certain elements to be evaluated under the conformity assessment procedure such as the technical documentation (Article 11 of the AI Act) and the DPIA, records of processing activities and other compliance measures under the GDPR.

Conformity Based on Assessment of Quality Management System and Assessment of Technical Documentation

(Annex VII)

REQUIREMENTS

Quality Management System

The provider must make an application to a notified body that includes:

a. The name and address of the provider and its authorised representative (if applicable);

b. The AI systems covered by the same quality management system;

c. The technical documentation for each AI system covered by the same quality management system;

d. The required quality management system documentation;

e. A description of the procedures in place to ensure that the quality management system remains adequate and effective; and

f. A written declaration that the same application has not been lodged with another notified body.

The notified body will assess the quality management system application and provide its assessment of the quality management system and the reasoned assessment decision.

The provider must notify any intended changes to the approved quality management system or the list of AI systems covered by the quality management system to the notified body. The proposed changes will be examined by the notified body to determine whether the modified quality management system remains satisfactory.

Control of the Technical Documentation

The provider must lodge an application with a notified body for the assessment of the AI systems' technical documentation, which must include:

a. The name and address of the provider;

b. A written declaration that the same application has not been lodged with another notified body; and

c. The technical documentation.

The notified body will examine the technical documentation. To the extent necessary, the notified body must be granted full access to the training, validation, and testing datasets used to enable it to perform its tasks.

The notified body may require the provider to produce further evidence or carry out further tests so as to enable a proper assessment of conformity of the AI system. If the notified body is not satisfied with the provider's tests, it may carry out its own tests.

Where it has not been possible to appropriately verify the AI system's conformity, the notified body must be granted access to the training and trained models of the AI system, including its relevant parameters.

The notified body's assessment decision will be notified to the provider. The decision will include its conclusions and a reasoned assessment decision.

Where the AI system is in conformity, an EU technical documentation assessment certificate shall be issued by the notified body. The certificate will include the conclusions of the examination, the conditions (if any) for its validity and the data necessary for the identification of the AI system. The certificate and its annexes shall contain all relevant information to allow for the evaluation of the conformity of the AI system. Where the AI system is not in conformity, the notified body will not issue an EU technical documentation assessment certificate and will inform the applicant accordingly, giving detailed reasons for its refusal.

The provider must notify any changes (whether intended or not) to the AI system that could affect its compliance with the requirements or its intended purpose, to the notified body that issued the certificate. The proposed changes will be examined by the notified body to determine whether the modified AI system remains satisfactory.

Surveillance of the Approved Quality Management System

The provider must allow the notified body to access the premises where the design, development, and testing of the AI systems is taking place, including sharing all necessary information.

The notified body will carry out periodic audits, including additional tests of the AI systems, to ensure the provider maintains and applies the quality management system.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems will need to establish processes and procedures to ensure the AI system's quality management system and technical documentation meet the requirements of the AI Act.

As part of this process, providers must ensure they engage and cooperate with the relevant notified bodies and submit quality management system and technical documentation applications to such bodies allowing them to properly assess the suitability of the quality management system(s) and technical documentation. A process must also be in place to ensure that any changes to the quality management system and/or technical documentation are provided to the relevant notified body.

INTERPLAY WITH THE GDPR

The GDPR does not include a conformity assessment procedure that businesses must follow. As such, businesses will not be able to leverage their GDPR compliance measures to address this requirement under the AI Act. However, there might be some interplay between certain elements to be evaluated under the conformity assessment procedure such as the technical documentation (Article 11 of the AI Act) and the DPIA, records of processing activities and other compliance measures under the GDPR.

EU Declaration of Conformity

(Article 47)

REQUIREMENTS

Before placing on the market or putting into service a high-risk AI system, the provider is required to draw up an EU declaration of conformity that is in writing, machine readable, and physically or electronically signed.

The EU declaration of conformity must be kept up-to-date, stored for 10 years and made available to national competent authorities upon request.

Providers are required to translate the EU declaration of conformity into a language that can be easily understood by the national competent authorities in the Member States in which they will place on the market or make available the AI system.

Annex V of the AI Act sets out the information elements that must be included in the EU declaration of conformity:

a. Name of the AI system and type, and any additional unambiguous reference allowing the identification and traceability of the AI system (e.g., serial number);

b. The name and address of the provider or, where applicable, its authorised representative;

c. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;

d. A statement warranting that the AI system is in compliance with the AI Act and, when applicable, other EU harmonisation legislation;

e. Where the AI system processes personal data, a statement that the AI system complies with the GDPR, the Law Enforcement Directive and EUDPR;

f. References to any relevant harmonised standards used or any other common specification in relation to which conformity is declared;

g. When a third-party conformity assessment procedure was undertaken (see page 39 of this Guide), the name and identification number of the notified body, a description of the conformity assessment procedure performed, and identification of the certificate issued; and

h. The place and date of issue of the declaration of conformity, the name and function of the person who signed it, as well as an indication for, or on behalf of, whom that person signed, as well as a signature.

For high-risk AI systems that are also subject to EU harmonisation legislation, a single declaration of conformity should be drafted covering all the applicable EU law.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems who are manufacturers of products subject to EU product safety legislation are likely familiar with this obligation and can leverage their experience.

Providers should ensure that they have the necessary resources to translate the EU declaration of conformity into a language or languages that can be understood by relevant national competent authorities. While some Member States may accept EU declarations of conformity written in English, a translation into the official language of the relevant Member State may still be required.

INTERPLAY WITH THE GDPR

The GDPR does not impose any similar obligations. However, it is important to note that, for AI systems processing personal data, businesses will be required to warrant their compliance with the GDPR (or other applicable EU data protection laws). Therefore, to comply with its obligations under the AI Act, businesses will be required to carry out an adequate evaluation of its AI system from a GDPR perspective.

CE Marking

(Article 48)

REQUIREMENTS

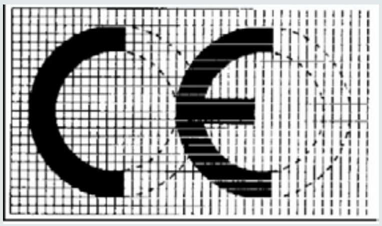
Providers are required to affix a CE marking to the high-risk AI system. This is a common obligation for products placed on the EU market. The CE marking must be affixed visibly, legibly, and indelibly. Where that is not possible, it must be affixed to the system's packaging or its accompanying documentation (see also Article 16(h) of the AI Act).

By doing so, the provider takes responsibility for the conformity of the product with the requirements under the AI Act and other applicable EU legislation requiring this marking in accordance with Article 30 of the Accreditation and Market Surveillance Regulation.

For high-risk AI systems provided digitally, a digital CE marking must be used, only if it can easily be accessed via the interface from which that system is accessed or via an easily accessible machine-readable code or other electronic means.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems who are manufacturers of products subject to EU product safety legislation are likely familiar with this obligation and can leverage their experience. Providers should refer to Annex II of the Accreditation and Market Surveillance Regulation for a graphical representation of the CE marking. For ease, this is set out below:



INTERPLAY WITH THE GDPR

The GDPR does not impose similar requirements.

Registration

(Article 49)

REQUIREMENTS

Before placing on the market or putting into service a high-risk AI system listed in Annex III of the AI Act (excluding high-risk AI systems intended to be used as safety components in the management and operation of critical infrastructure), providers shall register themselves and their system in the EU database of high-risk AI systems.

Registration obligations also apply to providers who concluded that their AI system is not high-risk following the assessment applicable under Article 6(3) of the AI Act (see Section 5 of this Guide).

High-risk AI systems intended to be used as safety components in the management and operation of critical infrastructure (Section 2 of Annex III of the AI Act) must be registered at national level.

PRACTICAL COMPLIANCE STEPS

Providers of AI systems listed in Annex III of the AI Act must ensure that they register themselves and their system in the EU database of high-risk AI systems (to be set up and maintained by the EU Commission), before placing the system on the market or putting it into service. The information to be submitted includes elements such as: (i) name, address, and contact details of the provider; (ii) description of the intended purpose of the AI system, its components, and the functions supported through the relevant AI system; and (iii) a basic and concise description of the information used by the system (data, inputs) and its operating logic (a more detailed list of required information is available in Annex VIII of the AI Act). Further information on the technical requirements for registration and specifications of the EU database is expected before the obligation to register becomes applicable.

Providers of high-risk AI systems intended to be used as safety components in the management and operation of critical infrastructure will need to register those systems at national level, not in the EU database. A country-specific analysis of the registration obligations in the relevant Member State(s) will be required for these systems.

INTERPLAY WITH THE GDPR

The GDPR does not impose registration requirements on businesses, except for certain registration requirements at a national level. That said, certain information maintained by the business to comply with the GDPR's accountability obligations (e.g., records of processing activities and DPIAs) may be leveraged for AI registration purposes.

Post-market Monitoring

(Article 72)

REQUIREMENTS

Providers must establish a post-market monitoring system that is proportionate to the nature and specific risks of their high-risk AI system.

The post-market monitoring system must actively and systematically collect, document and analyse relevant data on the performance of the concerned high-risk AI system throughout its lifetime. The performance data may be provided by deployers or collected through other sources. The post-marketing monitoring system should enable the provider to evaluate the continuous compliance of its AI system with the requirements set out in Chapter III, Section 2 of the AI Act (requirements for high-risk AI systems). Where relevant, post-market monitoring must include an analysis of the interaction with other AI systems.

The post-market monitoring system must be based on a post-market monitoring plan, which shall be part of the technical documentation referred to in Annex IV.

Providers of high-risk AI systems covered by Section A of Annex I of the AI Act may be able to leverage elements of the post-market monitoring systems implemented under Union harmonisation legislation.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems will need to establish and document a post-market monitoring plan aimed at collecting and reviewing experience gained from the use of AI systems they place on the market or put into service. The objective is to identify corrective or preventive actions that may be necessary to ensure continuous compliance. The post-market monitoring plan will need to be part of a provider's technical documentation. The EU Commission has an obligation to establish a template for such plan by 2 February 2026. Providers should monitor the Commission's activities in this respect and leverage the template once it becomes available.

As part of the monitoring plan, a post-market monitoring system will need to be implemented. This system should be designed to:

a. Collect, document, and analyse relevant data about the performance of the high-risk AI systems through their lifetime;

b. Allow the provider to evaluate continuous compliance of the high-risk AI systems with the requirements for such systems under the AI Act; and

c. Where relevant, analyse the interaction with other AI systems.

When developing the post-market monitoring system for AI, providers may consider looking to other areas with existing post-market surveillance requirements for inspiration (e.g., the medical device sector).

INTERPLAY WITH THE GDPR

The GDPR does not impose post-market monitoring requirements on businesses. As such, businesses will not be able to leverage their GDPR compliance measures to address this requirement under the AI Act. That said, certain continuous privacy risk assessment processes that have been implemented from a privacy-by-design perspective may be incorporated into the post-market monitoring system.

Incident Reporting

(Article 73)

REQUIREMENTS

Providers of high-risk AI systems must report all serious incidents to the MSA of the Member State where that incident occurred. A serious incident is any incident or malfunctioning of an AI system that leads to: (i) death or serious damage to a person's health, (ii) serious and irreversible disruption of critical infrastructure, (iii) a breach of EU law aimed at protecting fundamental rights, or (iv) serious damage to a property or the environment.

The MSA must be notified immediately after establishing a causal link (or the reasonable likelihood of such a link) between the AI system and the serious incident and, in any event, no later than 15 days after the provider becomes aware of the incident. Shorter notification timelines apply in the event of:

a. A widespread infringement or a serious incident leading to a serious and irreversible disruption of the management or operation of critical infrastructure (as defined in Article 3, point (49) (b) of the AI Act). In this case, the report must be provided immediately, and no later than 2 days after the provider becomes aware of that incident; and

b. The death of a person. In this case, the report must be provided immediately after the provider has established (or suspects) a causal link between the high-risk AI system and the serious incident, but no later than 10 days after the provider becomes aware of the serious incident.

To ensure timely reporting, the provider may submit an initial report that is incomplete, followed by a complete report.

Providers of high-risk AI systems that are already subject to serious incident reporting obligations under EU legislation listed in Annex III and providers of high-risk AI systems that are safety components of devices, or are themselves devices covered by EU medical device and in vitro medical device rules will only have to report incidents related to breaches of EU law aimed at protecting fundamental rights.

Following the reporting of a serious incident, the provider must, without undue delay, investigate the incident and the AI system concerned and implement any necessary corrective action. The provider shall cooperate with the competent authorities during its investigation.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems should develop, or revise existing, incident response policies and procedures to ensure they can meet the reporting requirements under the AI Act. The AI incident response policies and procedures should, among others, identify:

a. Mechanisms to detect, investigate, evaluate, and document incidents, including criteria to identify serious incidents that trigger reporting obligations. This may include providing information to deployers on how to recognise and report incidents related to the AI system;

b. Key steps in addressing any serious incidents that occur;

c. Responsible stakeholders for managing any serious incidents that occur;

d. The relevant authority(ies) that must be notified in the event of a serious incident; and

e. A timeline for reporting serious incidents, if necessary using a phased approach.

In addition to implementing and maintaining comprehensive incident response policies and procedures, providers should ensure that staff members receive appropriate training to detect and escalate incidents within the business.

INTERPLAY WITH THE GDPR

Pursuant to Article 33(1) of the GDPR, controllers have an obligation to notify personal data breaches to competent supervisory authorities unless the personal data breach is unlikely to result in a risk to individuals. This notification must be made without undue delay and, where feasible, no later than 72 hours after having become aware of the personal data breach. The measures and processes implemented to comply with GDPR breach response and notification obligations may be leveraged by providers to comply with incident reporting obligations under Article 73 of the AI Act.

Systems Subject to Specific Transparency Requirements

Type of businesses affected?

Providers (see Decision Tree 3 in Section 5 of this Guide).

Type of systems affected?

Systems subject to specific transparency requirements (see Decision Tree 2 in Section 5 of this Guide).

AI Systems Intended to Directly Interact with Individuals

(Article 50(1))

REQUIREMENTS

Providers of AI systems intended to directly interact with individuals must inform individuals about the fact that they are interacting with an AI system, unless it is obvious from the point of view of the individual that is reasonably well-informed, observant, and circumspect that this is the case, taking into account the circumstances and the context of use.

PRACTICAL COMPLIANCE STEPS

Providers of high-risk AI systems that are intended to directly interact with individuals (e.g., chatbots) should review their practices and products to ensure that it is clear to individuals that they are interacting with an AI system and that any information provided to individuals follows the rules under Article 50(5) of the AI Act.

INTERPLAY WITH THE GDPR

Although both the AI Act and the GDPR impose transparency requirements, the information/transparency requirements under the AI Act are substantially different from the transparency requirements applicable under the GDPR (e.g., Articles 13 and 14), and GDPR compliance measures will generally not be suitable for compliance with the requirement of Article 50(1) of the AI Act.

Content Generating AI Systems

(Article 50(2))

REQUIREMENTS

Providers of content generating AI systems must ensure that the outputs of their systems are marked in a machine-readable format and are detectable as artificially generated or manipulated. Providers must ensure that their technical solutions for marking outputs are effective, interoperable, robust, and reliable as far as this is technically feasible, taking into account specificities and limitations of different types of content, costs of implementation, and the generally acknowledged state-of-the-art, as may be reflected in relevant technical standards. This obligation does not apply to AI systems that perform an assistive function for standard editing or do not substantially alter the input data or the semantics provided by the deployer.

PRACTICAL COMPLIANCE STEPS

Providers of content generating AI systems should review their practices to ensure that it is clear to individuals that an output is artificially generated or manipulated and that any information provided to individuals follows the rules applicable under Article 50(5) of the AI Act.

INTERPLAY WITH THE GDPR

Although both the AI Act and the GDPR impose transparency requirements, the information/transparency requirements under the AI Act are substantially different from the transparency requirements applicable under the GDPR (e.g., Articles 13 and 14), and providers will not be able to leverage GDPR compliance work to comply with this AI Act requirement.

General Transparency

(Article 50(5))

REQUIREMENTS

The information must be provided in a clear and distinguishable manner at the latest at the time of the first interaction with or exposure to the AI system. The information must comply with applicable accessibility requirements (i.e., taking into account persons with disabilities).

PRACTICAL COMPLIANCE STEPS

Providers of AI systems subject to transparency requirements should review their transparency practices for their products to identify what information is being provided to users and when it is being provided. If the current practices are not in compliance with the relevant requirements, the provider should seek to address this. For example, the provider may implement new technical measures to ensure that the information is accessible or review the wording used to ensure that it is clear and understandable to users.

INTERPLAY WITH THE GDPR

The transparency requirements under the AI Act and the GDPR are substantially different. However, the level of transparency and clarity required, and the expected timing of such transparency, under each piece of legislation is similar. In instances where a provider is subject to both transparency requirements under the GDPR and the AI Act, it may be that it can inform individuals in compliance with both requirements (e.g., through a just-in-time notice).

General-purpose AI Models

Type of businesses affected?

Providers (see Decision Tree 3 in Section 5 of this Guide).

Type of models affected?

General-purpose AI models (see Decision Tree 2 in Section 5 of this Guide).

Obligations Applicable to All General-purpose AI Models

(Article 53)

REQUIREMENTS

Article 53 of the AI Act establishes a set of obligations applicable to all providers of general-purpose AI models. General-purpose AI models with systemic risk are subject to additional rules laid down by Article 55 of the AI Act.

Providers of general-purpose AI models are required to:

a. Prepare and keep up-to-date the technical documentation of the model, including its training and testing process and the results of its evaluation, and provide it to the AI Office or national authorities on request. The minimum details of the technical documentation are set forth in Annex XI of the AI Act;

b. Prepare, keep up-to-date, and make available information and documentation to providers of AI systems who intend to integrate the general-purpose AI model into their AI systems. This obligation is without prejudice to the need to protect intellectual property rights, trade secrets, and confidential business information. This information and documentation should allow providers of AI systems to have a good understanding of the capabilities and limitations of the general-purpose AI model to comply with their own obligations and contain the minimum elements set forth in Annex XII of the AI Act;

c. Implement a policy to comply with EU law on copyright and related rights; and

d. Prepare and make publicly available a sufficiently detailed summary of the content used for training of the general-purpose AI model, according to a template provided by the AI Office.

When they become available, providers of general-purpose AI models will be able to rely on codes of practice (Article 56 of the AI Act) and harmonised standards to demonstrate compliance with their obligations.

Providers of AI models that are released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available are exempt from the obligations referred in a) and b), unless these AI models qualify as general-purpose AI models with systemic risks.

PRACTICAL COMPLIANCE STEPS

Providers of general-purpose AI models will need to prepare new technical documentation that meets specific content requirements and ensure that providers of AI systems who intend to integrate the general-purpose AI model have the necessary information to comply with their own obligations under the AI Act (e.g., obligations related to high-risk AI systems).

Providers of general-purpose AI models will also be required to prepare and make publicly available a sufficiently detailed summary about the content used for training of the AI model. The AI Office will make available a template that providers should use to comply with this obligation.

These compliance elements will act as: (i) important accountability tools for providers of general-purpose AI models; (ii) key elements allowing providers of systems incorporating these models to understand them, deploy them correctly, and comply with their own obligations under the AI Act; and (iii) in the case of the detailed summary of elements used for training, a transparency tool that may also be useful for end-users in understanding the limitations of these models and exercising their rights when applicable.

In certain respects, the transparency element of the abovementioned obligations may be a challenge for providers of general-purpose AI models. Providers will have to balance the need to make information available to other providers and to end-users with their legitimate intellectual property rights, trade secrets, and confidential business information. Providers of general-purpose AI models should assess the best ways to comply with their obligations in a transparent manner while also protecting their rights (e.g., by putting in place NDAs with providers of AI systems who want to integrate the model).

Providers of general-purpose AI models should also assess whether the development of their model, particularly the training stage (post and pre-deployment), requires the use of copyrighted material. Based on this assessment, providers should develop and implement a policy to ensure that they comply with EU law on copyright and related rights. In this context, the AI Act highlights the need to deploy state-of-the-art technologies to identify and comply with reservations of rights introduced by rightsholders in their respective works.

INTERPLAY WITH THE GDPR

The obligations under Article 53 are fairly specific to the AI Act and have no immediate parallel with obligations under the GDPR. Businesses will need to develop new compliance documentation and processes to comply with this new requirement under the AI Act, unless an exception applies. That said, businesses may be able to leverage certain GDPR accountability efforts, such as the records of processing activities, when seeking to compile the information required to comply with the obligations under Article 53.

Authorised Representatives of Providers of General-purpose AI Models

(Article 54)

REQUIREMENTS

Before placing a general-purpose AI model on the EU market, providers established outside the EU must appoint a representative established in the EU through a written mandate. This obligation is applicable to both providers of regular general-purpose AI models and providers of general-purpose AI models with systemic risk.

The mandate should enable the representative, at a minimum, to:

a. Verify that the technical documentation specified in Annex XI has been drawn up and all obligations referred to in Article 53 and, where applicable, Article 55 have been fulfilled by the provider;

b. Keep a copy of the technical documentation specified in Annex XI at the disposal of the AI Office and national competent authorities, for a period of 10 years after the general-purpose AI model has been placed on the market, and the contact details of the provider that appointed the authorised representative;

c. Upon a reasoned request, provide the AI Office with all information and documentation necessary to demonstrate compliance; and

d. Upon a reasoned request, cooperate with the AI Office and competent authorities in any action they take in relation to the general-purpose AI model, including when the model is integrated into AI systems placed on the market or put into service in the EU.

The mandate should also enable the authorised representative to be addressed, in addition to or instead of the provider, by the AI Office or competent authorities, on all issues related to the compliance with the AI Act.

At the request of the AI Office, the authorised representative must provide a copy of the mandate in one of the official languages of the EU's institutions.

The authorised representative is also required to terminate the mandate if it considers that the provider is acting contrary to its obligations under the AI Act and to inform the AI Office of the termination and reasons for doing so.

Providers of AI models which are released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available, are exempt from the obligation to appoint a representative unless these AI models qualify as general-purpose AI models with systemic risks.

PRACTICAL COMPLIANCE STEPS

Businesses established outside the EU that intend to place a general-purpose AI model on the EU market should establish a relationship with an EU representative.

It is important that providers carefully select their representatives and establish a relationship of trust to ensure that both are able to act in a coordinated manner.

Representatives should also be technically capable to advise providers on any shortcomings regarding the technical documents or on the measures implemented by the provider to comply with its obligations under the AI Act.

INTERPLAY WITH THE GDPR

Similarly to Article 54 of the AI Act, Article 27 of the GDPR requires certain businesses established outside the EU but subject to the extraterritorial application of the GDPR to appoint an EU representative. While the specific tasks of the representative are different under the AI Act and the GDPR, the logic behind both the provisions is the same: having a point of contact in the EU capable of carrying out certain obligations and engaging with competent authorities. Businesses may even be able to appoint their current GDPR representatives as representatives under the AI Act if such representative has the technical capability to carry out the additional tasks established in the AI Act.

General-purpose AI Models with Systemic Risk

Type of businesses affected?

Providers (see Decision Tree 3 in Section 5 of this Guide).

Type of models affected?

General-purpose AI models with systemic risk (see Decision Tree 2 in Section 5 of this Guide).

Classification

(Articles 51 and 52)

REQUIREMENTS

In addition to the rules applicable to general-purpose AI models, the more advanced models will be classified as having a systemic risk and will be subject to more stringent requirements. A general-purpose AI model will be classified as a general-purpose AI model with systemic risk when:

a. It has high-impact capabilities which are evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks. A general-purpose AI model will be presumed to have high impact capabilities when the cumulative amount of computation used for its training is greater than 10^{25} FLOPs; or

b. It has capabilities or an impact equivalent to high impact capabilities considering the criteria set out in Annex XIII of the AI Act. Elements to be assessed under this Annex include, amongst others, the quality or size of the dataset, the amount of computation used for training the model, the benchmarks and evaluations of capabilities of the model, and the number of registered end-users.

The EU Commission may, in the future, adopt delegated acts to amend the thresholds for general-purpose AI models with systemic risks, as well as supplement benchmarks and indicators in light of evolving technological developments (such as algorithmic improvements or increased hardware efficiency).

When a provider becomes aware that its general-purpose AI model meets the requirements referred to above for high-impact capabilities, the provider is required to notify the EU Commission without delay and in any event within two weeks after that criteria is met or it becomes known that it will be met. The notification should include the information necessary to demonstrate that the relevant criteria has been met or substantiated arguments to demonstrate that, exceptionally, although the model meets the criteria, the general-purpose AI model does not present, due to its specific characteristics, systemic risks and should therefore not be classified as a general-purpose AI model with systemic risk.

Following the provider's notification, the EU Commission will issue a decision on whether the model should be classified as a general-purpose AI model with systemic risk. The EU Commission may also classify AI models as having a systemic risk *ex officio* or following a qualified alert from the scientific panel established under Article 68 of the AI Act.

PRACTICAL COMPLIANCE STEPS

Even though only a minority of general-purpose AI models are likely to be considered as presenting systemic risks, providers should have a process in place to monitor the capabilities, computing power used for training, and other characteristics of their general-purpose AI models. If any of their general-purpose AI models exceeds the legal threshold set forth under the AI Act, providers should have procedures in place to ensure prompt notification to the EU Commission. General-purpose AI models with systemic risk will be subject to a number of additional obligations which are analysed in further details in the next pages of this Guide.

INTERPLAY WITH THE GDPR

There is no immediate parallel in the GDPR to the mechanism for classification of general-purpose AI systems with systemic risk nor to the classification procedure supporting it.

However, certain GDPR compliance measures, particularly the measures related to prior consultation with the Supervisory Authorities following a DPIA (Article 36 of the GDPR) can serve as a basis to design the necessary procedures for notification and engagement with the EU Commission under the AI Act.

Obligations of General-purpose AI Models with Systemic Risk
(Article 55)

REQUIREMENTS

General-purpose AI models with systemic risk are subject to the obligations applicable to regular general-purpose AI models (see page 48 of this Guide), and an additional set of obligations set out in Article 55 of the AI Act. These specific obligations require providers of general-purpose AI models with systemic risk to:

a. Perform model evaluation in accordance with standardised protocols and tools reflecting the state of the art, including conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks;

b. Assess and mitigate possible systemic risks at EU level, including their sources, that may stem from the development, the placing on the market, or the use of general-purpose AI models with systemic risk;

c. Keep track of, document, and report, without undue delay, to the AI Office and, as appropriate, to national competent authorities, relevant information about serious incidents and possible corrective measures to address them; and

d. Ensure an adequate level of cybersecurity protection for the model and the physical infrastructure of the model.

Similar to general-purpose AI models, providers of general-purpose AI models with systemic risks will be able to rely on codes of practice (Article 56 of the AI Act) and harmonised standards to demonstrate compliance with their obligations, when they become available.

PRACTICAL COMPLIANCE STEPS

The AI Act's risk-based approach extends also to the regulation of general-purpose AI models.

Accordingly, providers of general-purpose AI models with systemic risk will have to put in place a more robust compliance programme and deploy additional resources, by comparison to providers of "regular" general-purpose AI models. In particular, providers of general-purpose AI models with systemic risk will need to ensure that they have in place the necessary technical measures for adequate model evaluation and assessment and mitigation of systemic risk.

Additionally, such providers will be required to take steps to ensure both the cybersecurity of the general-purpose AI model and that of the model's physical infrastructure.

Finally, providers of general-purpose AI models with systemic risks will have to implement the necessary measures to ensure prompt documentation and reporting of information about serious incidents and corrective measures aimed at addressing them.

INTERPLAY WITH THE GDPR

⊖

As with the obligations under Article 53 of the AI Act for "regular" general-purpose AI models, the obligations applicable to general-purpose AI models with systemic risk are specific to the AI Act.

That said, some parallels may be drawn between the obligations set out in Article 53 of the AI Act and those of the GDPR related to security and breach notification. Businesses can leverage their GDPR frameworks for data security and cybersecurity and extend them to general-purpose AI models and the models' physical infrastructure. With respect to incident reporting, businesses can expand their GDPR breach reporting systems to include AI-specific incidents. Coordination between DPOs or individuals in charge of privacy and data protection and those responsible for AI compliance will ensure that all reporting obligations are met efficiently. Businesses subject to the GDPR are required to conduct DPIAs for high-risk data processing activities and such businesses can build on their DPIA processes to conduct comprehensive risk assessments for AI models. This includes evaluating potential systemic risks associated with general-purpose AI models and implementing mitigation strategies in line with both GDPR and AI Act requirements.

8. Practical Obligations for Businesses: Deployer Obligations

High-risk AI Systems

Type of businesses affected?

Deployers (see Decision Tree 3 in Section 5 of this Guide).

Type of systems affected?

High-risk AI systems (see Decision Tree 2 in Section 5 of this Guide).

Complying with the Instructions of the Provider

(Article 26(1))

REQUIREMENTS

Deployers of high-risk AI systems are required to take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use that accompany the AI system.

PRACTICAL COMPLIANCE STEPS

Deployers will need to assess whether AI systems they use are designated as high risk, and assess the particular risks associated with the use of those systems. Based on those risks, they will need to implement appropriate internal policies, processes, and technical controls to ensure that the AI systems are used in accordance with any instructions of the provider.

From an accountability perspective, deployers should consider keeping an up-to-date register of high-risk AI systems used by the business and the providers' instructions for use of the respective systems. In addition, deployers should ensure that the responsibility to monitor compliance with the providers' instructions is allocated to an appropriate function or committee within the business (e.g., a multidisciplinary AI governance committee).

Further, deployers should implement measures to ensure that they are aware of any changes in the instructions with respect to the high-risk AI systems they use (e.g., by including appropriate notification obligations in agreements with high-risk AI system providers).

INTERPLAY WITH THE GDPR

Under Article 24 of the GDPR, controllers are required to implement appropriate technical and organisational measures to ensure and to be able to demonstrate compliance with the GDPR. This is similar to the deployers' accountability obligation described above in relation to compliance with providers' instructions for use of high-risk AI systems. Where high-risk AI systems involve personal data processing, deployers will likely need to implement policies and procedures that address their accountability obligations under both the GDPR and the AI Act. Furthermore, deployers may consider leveraging their GDPR accountability framework for AI accountability purposes.

Oversight Obligations

(Article 26(2))

REQUIREMENTS

Deployers of high-risk AI systems must assign human oversight over the use of such systems to individuals who have the necessary competence, training, authority and support to do so.

PRACTICAL COMPLIANCE STEPS

Deployers will need to identify an appropriate individual or group of individuals within the business to oversee the use of high-risk AI systems, ensure these individuals have the appropriate authority to exercise oversight, and are provided with the appropriate training and resources to do so. For some businesses, the function or committee responsible for overseeing compliance with the provider's instructions regarding the use of the high-risk AI system (as required by Article 26(1) of the AI Act) may be well-placed to provide human oversight.

The individuals to whom the human oversight responsibility is allocated should have the knowledge, tools, and resources to:

a. Properly understand the capacities and limitations of the system and be able to monitor its operation to detect and address anomalies, dysfunctions, and unexpected performance;

b. Remain aware of the possible tendency to automatically rely or over-rely on the output of the system (so called, automation bias);

c. Correctly interpret the system's output;

d. Decide not to use the system or to disregard, override or reverse the system's output in a particular situation; and

e. Intervene in the system's operation or interrupt it, through a stop button or similar procedure that brings the system to a halt in a safe state.

INTERPLAY WITH THE GDPR

The GDPR requires businesses in certain circumstances to appoint a DPO responsible for overseeing compliance with the GDPR. Where deployers use high-risk AI systems that involve processing of personal data, they may need to appoint a DPO. Depending on the particular situation, it may be appropriate to have the DPO coordinate or closely cooperate with the individuals or teams responsible for ensuring human oversight over the high-risk AI system(s). In particular, the DPO can provide relevant background and training considering the experience accumulated from compliance with the rules on automated decision-making under the GDPR.

Data Management

(Article 26(4))

REQUIREMENTS

If a deployer of a high-risk AI system exercises control over the input data, it must ensure that the input data is relevant and sufficiently representative, in light of the intended purpose of the high-risk AI system.

PRACTICAL COMPLIANCE STEPS

Before adding input data to a high-risk AI system, providers will need to evaluate that data to determine whether it is fit for purpose, based on its relevance and representativeness (i.e., accurate and without bias), for the purpose of the system.

INTERPLAY WITH THE GDPR

The obligation under the AI Act to ensure that input data is relevant and representative for the intended purpose of the AI system overlaps with businesses' obligations under the GDPR's data minimisation and accuracy principles. Although the scope of the obligation under the AI Act is not limited to personal data, businesses may be able to leverage the data protection by design and by default measures of their GDPR compliance program to comply with the obligation under the AI Act to exercise control over input data.

Monitoring

(Article 26(5))

REQUIREMENTS

Deployers of high-risk AI systems are required to carry out ongoing monitoring of the operation of high-risk AI systems on the basis of the instructions for use provided by the provider, and where relevant, inform providers in accordance with Article 72 of the AI Act (Post-market monitoring). Where a risk within the meaning of Article 79(1) of the AI Act (i.e., a risk to the health and safety or fundamental rights of individuals) is identified by the deployer, the deployer must, without undue delay (i) inform the provider or distributor, (ii) inform the relevant MSA, and (iii) suspend use of the system. Where a deployer identifies a serious incident, it must also immediately inform the first provider, then the importer or distributor and the relevant MSA of the incident.

PRACTICAL COMPLIANCE STEPS

Deployers will need to establish internal policies and procedures to monitor usage of high-risk AI systems and to identify any risks that arise as a result of its use. In addition, deployers will need to ensure that sufficient planning and internal processes are in place to notify relevant parties of risks that arise within the requisite time frames. Deployers should also consider whether existing policies (e.g., an incident response policy) require updates to allow for compliance with the AI Act.

INTERPLAY WITH THE GDPR

The obligation under the AI Act is new and does not have an overlap with an existing obligation under the GDPR. Businesses will not be able to leverage GDPR compliance measures to comply with the concerned requirement under the AI Act.

Maintain Logs Automatically Generated by the High-risk AI System

(Article 26(6))

REQUIREMENTS

Deployers of high-risk AI systems are required to keep logs generated by the system, to the extent such logs are in their control.

The logs must be maintained for a period appropriate to the intended purpose of the system, but at least for six months, and subject to applicable EU or Member State law, in particular data protection laws.

PRACTICAL COMPLIANCE STEPS

Deployers will need to ensure that logs generated are retained for a period that is relevant to the intended purpose of the system, taking into account any data retention obligations that exist under data protection laws.

INTERPLAY WITH THE GDPR

If logs include personal data, deployers will need to carefully balance retention periods to ensure that logs are retained for a sufficient period to comply with AI Act, but that personal data is not retained for longer than is strictly necessary in accordance with the GDPR's storage limitation principle.

Transparency with Employees

(Article 26(7))

REQUIREMENTS

Before deploying high-risk AI systems in the workplace, deployers who are employers are required to inform workers' representatives and any impacted workers of the system, in accordance with relevant rules and procedures set out in EU or Member State law.

PRACTICAL COMPLIANCE STEPS

Deployers will need to consult with workers' representatives in certain circumstances.

INTERPLAY WITH THE GDPR

In many Member States, deployers are subject to obligations to inform or consult with workers' representatives when introducing new personal data processing activities that impact employees. In many cases, those obligations will be triggered in the same circumstances as the workers' representative consultation requirement under the AI Act described above, and it may be appropriate for deployers to address both consultation obligations simultaneously.

Data Protection Impact Assessment

(Article 26(9))

REQUIREMENTS

Where relevant, deployers of high-risk AI systems must use the information provided to them pursuant to Article 13 of the AI Act (Transparency and Provision of Information to Deployers) to comply with their obligation to carry out a DPIA under Article 35 of the GDPR.

PRACTICAL COMPLIANCE STEPS

Deployers will need to update existing DPIA templates to incorporate relevant issues regarding the processing of personal data in high-risk AI systems.

INTERPLAY WITH THE GDPR

In many cases, the use of high-risk AI systems will trigger the requirement to carry out a DPIA under Article 35 of the GDPR, and the AI Act specifically requires certain information provided to the deployer under the AI Act to be incorporated into that process.

Inform Individual of Use of Decision-making AI System

(Article 26(11))

REQUIREMENTS

Deployers of high-risk AI systems of the type referred to in Annex III that make decisions, or assist in making decisions, with respect to individuals, are required to inform those individuals that they are subject to the use of a high-risk AI system.

PRACTICAL COMPLIANCE STEPS

Deployers will need to understand whether an AI system will be used to make decisions, or assist in making decisions, about individuals. Deployers should consider preparing template language that can be used to inform individuals.

INTERPLAY WITH THE GDPR

When a high-risk AI system involves making decisions that impact individuals, such will frequently trigger relevant obligations under the GDPR in respect of automated decision making that has a material impact on individuals. In those circumstances, the GDPR requires businesses to inform individuals of automated decision-making, provide meaningful information about the logic involved, and explain the significance and envisaged consequences of the automated decision-making. Businesses will also likely be subject to the rules on provision of information under Articles 13 and 14 of the GDPR. With this in mind, businesses will be able to leverage their GDPR compliance efforts for compliance with the AI Act requirements.

Cooperation with Competent Authorities

(Article 26(12))

REQUIREMENTS

Deployers of high-risk AI systems must cooperate with relevant competent authorities in any action taken in relation to such systems.

PRACTICAL COMPLIANCE STEPS

To assist in complying with such cooperation obligations, deployers should consider:

a. Establishing internal procedures for responding to requests and inquiries from competent authorities;

b. Designating a point of contact with responsibility for liaising with competent authorities;

c. Training relevant personnel on their obligations and procedures for cooperation with competent authorities; and

d. Maintaining comprehensive documentation related to AI systems in use and ensuring such documentation is appropriately filed and available upon request.

INTERPLAY WITH THE GDPR

Article 31 of the GDPR requires both controllers and processors to cooperate, on request, with DPAs in the performance of their tasks. This obligation extends to the provision of information necessary to demonstrate compliance with the GDPR and cooperation with investigations conducted by a DPA and is similar to the cooperation obligations established in the AI Act. While requests for cooperation made under the GDPR and AI Act are likely to be different in practice, businesses will likely be able to leverage any GDPR cooperation procedures and mechanisms for the purpose of complying with the cooperation obligations under the AI Act. This will be particularly helpful in countries where the DPA is also appointed as the MSA under the AI Act

Fundamental Rights Impact Assessment for High-risk AI Systems (Article 27)

REQUIREMENTS

Prior to deploying high-risk AI systems that evaluate the creditworthiness of individuals or establish their credit score (Annex III(5)(b)) or for risk assessment and pricing in relation to individuals in the case of life and health insurance (Annex III(5)(c)), deployers are required to carry out an assessment of the impact on fundamental rights of individuals that may be produced by the system. Additional high-risk AI systems may be subject to this obligation when deployed by bodies governed by public law or private entities providing public services. The fundamental rights impact assessment must include:

a. A description of the deployer's processes in which the system will be used in accordance with its intended purpose;

b. A description of the time period in which, and the frequency with which, the system will be used;

c. The categories of individuals and groups likely to be affected by use of the system;

d. The specific risks of harm likely to have an impact on the concerned individuals, taking into account information provided by the provider pursuant to Article 13 of the AI Act;

e. A description of human oversight measures implemented, in accordance with the instructions for use of the provider; and

f. Measures to be taken where identified risks materialise, including internal governance arrangements and complaint mechanisms.

The obligation referred to above is applicable to the first use of a high-risk AI system. Accordingly, a deployer may rely on previously conducted assessments carried out by the provider. However, to the extent any of the elements described above change during use of the system, the deployer is required to update the assessment.

Deployers are required to notify the relevant MSA of the results of the assessment, using the template that will be published by the AI Office.

Where the information required in a fundamental rights assessment is already covered in a DPIA, the fundamental rights assessment shall complement the DPIA.

PRACTICAL COMPLIANCE STEPS

Deployers will need to implement internal processes to ensure that any required fundamental rights assessments are carried out and updated if necessary, as well as to ensure that the appropriate filing is made to the MSA.

As a practical matter, the individual or team designated to oversee the high-risk AI system pursuant to Article 26 of the AI Act should likely be closely involved in this process and, if they have the necessary resources and capabilities, may assume a leading role.

INTERPLAY WITH THE GDPR

In many cases there is likely to be a substantial overlap between the obligation to carry out a fundamental rights assessment under the AI Act and the obligation to carry out a DPIA under the GDPR. In addition, much of the information included in each assessment will be the same or similar. In practice, businesses will likely be able to adopt internal processes that address both sets of requirements simultaneously.

Right to Explanation of Individual Decision-making

(Article 86)

REQUIREMENTS

Any person subject to a decision which:

a. Is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III of the AI Act (with the exception of systems intended to be used as safety components in the management and operation of critical infrastructure and systems in relation to which this obligation is restricted by EU or Member State law); and

b. Produces legal effects or similarly significantly affects them in a way that they consider to adversely impact their health, safety, and fundamental rights;

shall have the right to request from the deployer clear and meaningful explanations on the role of the AI system in the decision-making procedure and the main elements of the decision taken.

PRACTICAL COMPLIANCE STEPS

Deployers will need to determine whether an AI system will be used to make decisions, or assist in making decisions, about individuals. In addition, deployers will need to understand how the AI system actually plays its part in making the decision. In practice, deployers must ensure that they are able to provide a meaningful explanation regarding the decision-making process of the AI system to individuals, when requested. This may require the deployer to seek assistance of the provider of the AI system or to ensure that the system is set up in a way that it can easily generate an explanation of the decision-making process when it is requested.

INTERPLAY WITH THE GDPR

Under the GDPR, businesses are required to inform individuals of automated decision-making, provide meaningful information about the logic involved, and explain the significance and envisaged consequences of the automated decision-making. The GDPR also contains the right of access under Article 15 which permits the individual to request this information again. Businesses can leverage their GDPR compliance efforts for compliance with the AI Act requirements.

Systems Subject to Specific Transparency Requirements

Type of businesses affected?

Deployers (see Decision Tree 3 in Section 5 of this Guide).

Type of systems affected?

Systems subject to specific transparency requirements (see Decision Tree 2 in Section 5 of this Guide).

Emotion Recognition and Biometric Categorisation Systems

(Article 50(3))

REQUIREMENTS

Deployers of emotion recognition and biometric categorisation systems must inform persons exposed to them of their operation, and must ensure that any related personal data processing is carried out in accordance with the GDPR.

PRACTICAL COMPLIANCE STEPS

Deployers of emotion recognition and biometric categorisation systems should review their practices and products to ensure that it is clear to individuals that they are interacting with an AI system.

Deployers will need to consider preparing clear notice language that is presented in a distinguishable manner, at the latest at the time of the first interaction with or exposure of an individual to the AI system. This could be achieved, for example, through the use of pop-ups or banners, in an online contex, or signs in an offline context.

INTERPLAY WITH THE GDPR

⊖ Although both the AI Act and the GDPR impose transparency requirements, the information and transparency requirements under the AI Act are substantially different from those applicable under the GDPR (Articles 13 and 14 of the GDPR) and GDPR compliance measures will generally not be suitable for compliance with the requirement under the AI Act. However, in instances where a deployer is subject to both transparency requirements under the GDPR and the AI Act, it may be able to inform individuals in compliance with both requirements simultaneously (e.g., by combining information to be provided under the GDPR and the AI Act in a first layer notice).

AI Systems that Generate or Manipulate Images, Audio, Video, or Text

(Article 50(4))

REQUIREMENTS

Deployers of systems that generate or manipulate image, audio, or video content constituting a deep fake must disclose that the content has been artificially generated or manipulated. Where such content forms part of an evidently artistic, creative, satirical, or fictional work, these obligations are limited to disclosure of the existence of manipulated or generated content in a manner that does not prejudice the display or enjoyment of the work.

Deployers of AI systems that generate or manipulate text that will be published for the purpose of informing the public of matters of public interest must also disclose that the work has been artificially generated or manipulated, unless the AI-generated content has undergone a process of human review or editorial control and a person holds editorial responsibility for the publication of the content.

PRACTICAL COMPLIANCE STEPS

Deployers of AI systems that generate or manipulate images, audio, video content, or text, should review their practices and products to ensure that it is clear to individuals that they are interacting with an AI system. This can, for example, be achieved by labelling the content or including a clear warning message that is displayed when the individual first interacts with or is exposed to the content (e.g., a warning message at the beginning of a video). For text-based deepfakes, appropriate transparency could be achieved through, for example, a disclaimer at the top of the text.

INTERPLAY WITH THE GDPR

Although both the AI Act and the GDPR impose transparency requirements, the information and transparency requirements under the AI Act are substantially different from the transparency requirements applicable under the GDPR (Articles 13 and 14 of the GDPR) and GDPR compliance measures will generally not be suitable for compliance with the requirement under the AI Act. However, in instances where a deployer is subject to both transparency requirements under the GDPR and the AI Act, it may be able to inform individuals in compliance with both requirements simultaneously.

General Transparency

(Article 50(5))

REQUIREMENTS

The information must be provided in a clear and distinguishable manner at the latest at the time of the first interaction with or exposure to the AI system. The information must comply with applicable accessibility requirements (i.e., taking into account persons with disabilities).

PRACTICAL COMPLIANCE STEPS

Deployers of AI systems subject to transparency requirements should review what information is being provided to users and when it is being provided in respect of their providers. If the current practices are not in compliance with the relevant requirements, the deployer should seek to address this. For example, the provider may implement new technical measures to ensure that the information is accessible or review the wording used to ensure that it is clear and understandable to users.

INTERPLAY WITH THE GDPR

As noted above, the transparency requirements under the AI Act and the GDPR are substantially different. However, the level of transparency and clarity required, and the expected timing of such transparency, under each piece of legislation is similar. In instances where a deployer is subject to both transparency requirements under the GDPR and the AI Act, it may be able to inform individuals in compliance with both requirements simultaneously (e.g., through a just-in-time notice).

9. Supervision and Enforcement

In this section, we provide an overview of the authorities and bodies that will be competent to oversee compliance with the AI Act at Member State and EU level, as well as a summary of their enforcement powers.

Supervision

Member State Level

The AI Act requires that each Member State designates at least one "notifying authority" and at least one MSA as "national competent authorities" for the purposes of overseeing the application and implementation of the AI Act. Member States are free to decide to set up new authorities or to designate existing authorities as national competent authorities under the AI Act. Member States must ensure that the national competent authorities are provided with adequate technical, financial and human resources, and with the infrastructure, to fulfil their tasks under the AI Act.

The notifying authority and MSA have different responsibilities and roles, as discussed further below. However, some tasks are common, such as providing guidance and advice as to the implementation of the AI Act. Businesses are required to cooperate with both national competent authorities.

All businesses subject to the AI Act should be aware of the Member State authorities that will regulate their use of an AI system. How Member States opt to structure national competent authorities may differ, so it is important that businesses familiarise themselves with the relevant national authorities that are competent to oversee their AI-related activities. As with the GDPR, this may include an authority in a country where the business itself is not located.

Notifying Authority

The primary role of the notifying authority is to set up and carry out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for compliance monitoring of their activities. These procedures must be developed in cooperation with the notifying authorities of the other EU Member States. Notifying authorities must notify the EU Commission and other Member States of each conformity assessment body that satisfies the requirements of the AI Act. Existing national notifying authorities exercising competences in the context of the single market compliance space, particularly in fields such as machinery, may be well-placed to take on the role of notifying authority under the AI Act.

MSA

Whereas the notifying authorities' role is focused on the conformity assessment procedure, MSAs will have a broader role in overseeing compliance by providers, deployers and other entities in the AI value chain. To carry out this task, MSAs are given the extensive powers of market surveillance, investigation and enforcement established in Article 14 of the Market Surveillance Regulation, including the power to: (i) require businesses to provide the MSA with the materials and information necessary to conduct an investigation; (ii) conduct unannounced on-site inspections and physical checks of products (including AI systems); (iii) issue orders requiring businesses to bring their practices into compliance; (iv) take appropriate corrective actions, including prohibiting or restricting the making available of a product on the market or to order that the product is withdrawn or recalled; and (v) impose penalties (as detailed further below).

Member States must designate one MSA to act as single point of contact for the AI Act in their jurisdiction and the EU Commission will publish a list of the single points of contact.

The AI Act contains specific obligations which are owed to the MSAs by businesses. For example, the deployer must notify the MSA of the results of a fundamental rights impact assessment, and providers of high-risk AI systems must report any serious incidents to the MSA. The AI Act also confers rights to MSAs, such as to approve any plans for real-world testing of high-risk AI systems by providers, and to carry out an evaluation of an AI system which the relevant MSA has sufficient reason to believe presents a risk, or where it believes an AI system classified as not high-risk is, in fact, high-risk. The AI Act also sets out compliance obligations for MSAs, such as reporting to the EU Commission annually on any information identified in the course of market surveillance activities that may be of interest for the application of EU competition law, and information about the use of prohibited practices.

The EDPS will take the role of MSA for overseeing the EU bodies' use of AI systems. Similarly, some national data protection authorities have indicated that they are well placed to take on the MSA role in their respective Member State. Other authorities, such as consumer protection and/or competition authorities may also be willing to take up this role.

EU Level

AI Office

The AI Act introduces the AI Office which was established by a EU Commission Decision of 24 January 2024. The mission of the AI Office is to develop EU expertise and capabilities in the field of AI and to contribute to the implementation of EU law on AI. It is also responsible for the supervision and enforcement of requirements in respect of general-purpose AI models.

The AI Office will produce documentation and take other steps that are informative and applicable for all businesses subject to the AI Act. Therefore businesses should monitor the publications and activities of the AI Office. From a compliance perspective, the AI Office will be of particular significance to providers of general-purpose AI models.

AI Board

The AI Act introduces and establishes the AI Board. The AI Board is comprised of one representative per EU Member State and its mission is to advise and assist the EU Commission and the Member States in order to facilitate the consistent and effective application of the AI Act. Relevant tasks of the AI Board include:

- Collecting and sharing of technical and regulatory expertise and best practices among Member States;
- Issuing recommendations and written opinions on matters related to the implementation of the AI Act and its consistent and effective application; and
- Supporting the EU Commission in promoting AI literacy, public awareness and understanding of the benefits, risks, safeguards, rights, and obligations in relation to the use of AI systems.

The AI Board will perform functions similar to the EDPB under the GDPR, such as producing guidance. However, the AI Board lacks the extensive dispute resolution powers of the EDPB. All businesses should monitor publications and other activities of the AI Board, and take these into consideration where relevant.

The EU Commission

The EU Commission has a number of responsibilities and tasks throughout the AI Act, such as preparing certain documentation, adopting delegated acts, and setting up and maintaining the database for high-risk AI systems.

Enforcement Powers

In addition to investigative and corrective powers, MSAs have the power to impose fines. The AI Act contains the following levels of fines depending on the type of infringement:

- €35 million or 7% of total worldwide annual turnover for the preceding year, whichever is higher, for non-compliance with the rules around prohibited AI practices;
- €15 million or 3% of total worldwide annual turnover for the preceding year, whichever is higher, for non-compliance with most obligations under the AI Act; and
- €7.5 million or 1% of total worldwide annual turnover for the preceding year, whichever is higher, for the supply of incorrect, incomplete or misleading information.

MSAs will consider all relevant circumstances of a specific situation when deciding whether to impose an administrative fine and, if so, the amount of the fine, such as the nature, gravity, and duration of the infringement and of its consequences, and the intentional or negligent character of the infringement. In addition to the abovementioned fines, Member States can also establish additional rules on penalties and other enforcement measures, which may include warnings and non-monetary measures. Businesses should identify specific enforcement rules implemented at Member State level in relevant jurisdictions.

Distinct from the fines listed above, the EU Commission has the power to impose fines on providers of general-purpose AI models. Specifically, it may impose a fine of €15 million or 3% of total worldwide annual turnover for the preceding year, whichever is higher.

Fines under the AI Act are structured similarly to the GDPR in that they are based on the nature of the infringement. A business subject to a fine under the AI Act could also be subject to a fine under the GDPR if the relevant activities involve the processing of personal data in violation of the GDPR.

Complaints

Natural or legal persons may submit a complaint to their MSA if they consider that an infringement of the AI Act has taken place.

10. Glossary

The following terms and abbreviations are used in this Guide:

Accessibility Directives: Directive 2019/882/EU of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services and Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies.

Accreditation and Market Surveillance Regulation: Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

AI Act: Regulation EU 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

AI Board: The European Artificial Intelligence Board.

AI Liability Directive: Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence.

AI Office: The AI Office which was established by a Commission Decision of 24 January 2024 to support implementation of the AI Act and to enforce its rules on general purpose AI models.

CJEU: The Court of Justice of the EU.

Controller: The entity that determines the purposes and means of the processing of personal data, within the meaning of Article 4(7) of the GDPR.

Copyright Directive: Directive 2019/790/EU of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

Council: The Council of the EU.

Cyber Resilience Act: Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

Cybersecurity Act: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

Digital Services Act: Regulation 2022/2065/EU of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC.

DPA: A Data Protection Supervisory Authority under the GDPR.

DPIA: A Data Protection Impact Assessment, within the meaning of Article 35 of the GDPR.

DPO: A Data Protection Officer, within the meaning of Chapter IV, Section 4 of the GDPR.

EDPB: The European Data Protection Board, an EU-level body composed of the data protection authorities of all EU Member States created under Chapter VII, Section 3 of the GDPR to oversee its implementation and enforcement and to issue guidance.

EDPS: The European Data Protection Supervisor, the EU independent data protection authority, responsible for overseeing the compliance of EU institutions and agencies with data protection laws.

EU: The European Union.

EU Commission: The European Commission.

EUDPR: Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

EU Parliament: The European Parliament.

GDPR: Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Law Enforcement Directive: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Member States: The Member States of the EU.

MSA: The Market Surveillance Authority under the AI Act.

Market Surveillance Regulation: Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC).

Personal Data: Information relating to an identified or identifiable individual, within the meaning of Article 4(1) of the GDPR.

Processor: An entity that processes personal data on behalf of the controller, within the meaning of Article 4(8) of the GDPR.

Product Liability Directive: Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.

Standardisation Regulation: Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.

UK: The United Kingdom.

11. Key Contacts

Leadership

David Dumont

Partner | Brussels | ddumont@Hunton.com

David is a partner in the firm's Brussels office. He assists large, multinational clients with various aspects of EU privacy, data protection, and cybersecurity laws, including working extensively with clients on compliance with the GDPR and new EU digital laws such as the AI Act, the NIS2 Directive, and DORA. In addition to managing global compliance projects, David advises clients on cutting-edge privacy and data protection issues, including AI technologies and applications. He also has helped numerous clients implement mechanisms to legitimize international data flows, such as EU Standard Contractual Clauses and Binding Corporate Rules.

Sarah Pearce

Partner | London | spearce@Hunton.com

Sarah is a partner in the firm's London office. Her practice covers a broad range of data privacy and data security issues in the UK and across Europe. Ranked by *Chambers and Partners UK*, she has extensive experience advising clients on UK/EU privacy, UK/EU data protection and cybersecurity compliance issues, including those associated with international data transfers, conducting privacy impact assessments, and risk management associated with the collection and use of data (particularly in the context of leading-edge technologies such as AI) and marketing-related issues. Sarah also advises clients on cybersecurity incident response and associated regulatory investigations and enforcement proceedings.

Lisa Sotto

Partner | New York | lsotto@Hunton.com

Lisa is the global head of the firm's Privacy and Cybersecurity practice. Well-known in the field as a "legend" and "market leader," Lisa is ranked as the only "Star Individual" for privacy, and data security by *Chambers and Partners*, and is recognized in the Hall of Fame for cyber law, privacy and data protection by *Legal 500*. *Chambers and Partners* honored Lisa with the 2021 Outstanding Contribution to the Legal Profession award, which is given to only one lawyer each year for exceptional achievements. Appointed by Secretaries Mayorkas, Nielson, Johnson, and Napolitano, Lisa serves as Chair of the US Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Aaron Simpson

Partner | New York and London | asimpson@Hunton.com

Aaron, a partner in the firm's New York office, has more than 20 years of experience advising clients on a broad range of complex global privacy, data protection, and cybersecurity matters, including with respect to existing and emerging requirements in the US and EU. He offers broad and unique transatlantic experience, having lived and worked in both our New York and London offices. Recognized by *Chambers and Partners USA* and *Legal 500*, Aaron's work includes advising clients on large-scale cybersecurity incidents; conducting diligence and negotiating privacy and data security aspects of corporate transactions; developing of cross-border data transfer solutions; developing local, regional, and international privacy and data protection compliance programs; and negotiating data-driven commercial agreements.

Brittany Bacon

Partner | New York | bbacon@Hunton.com

Brittany is a partner in the firm's New York office. Ranked in *Chambers and Partners USA*, *Legal 500*, *New York Law Journal*, and "40 under 40" by *Global Data Review*. Brittany is recognized widely as a leading lawyer for privacy and cybersecurity. Brittany assists clients in identifying, evaluating, and managing privacy and information security risks and compliance issues. She also builds global privacy programmes designed to comply with domestic and foreign legal requirements, including US state privacy laws and the EU GDPR. She routinely conducts privacy impact assessments and advises companies on managing risk in connection with extensive and innovative data collection and use and global marketing programmes. Brittany also advises large, multinational companies on catastrophic cybersecurity incidents.

Michael La Marca

Partner | New York | mlamarca@Hunton.com

Mike is a partner in the firm's New York office. Mike advises multinational clients on compliance with all federal, state and international privacy and data security laws, and managing privacy and cybersecurity risks and policy issues. His work includes analysing and advising on US state biometric privacy and surveillance law implications. He also regularly assists companies engaged in cutting-edge technologies and information practices, such as AI/machine learning, biometrics, geolocation tracking, and Internet of Things devices.

Adam Solomon

Partner | New York | asolomon@Hunton.com

Adam is a partner in the firm's New York office. Adam regularly advises clients on all legal issues associated with information security programs, cybersecurity incidents, and electronic surveillance practices. He assists clients in identifying, evaluating, and managing global privacy and information security risks and compliance issues. Adam has experience negotiating a wide range of technology and data licensing agreements, and drafting information security policies and standards, incident response plans, website and mobile app terms of use, privacy notices, and nondisclosure agreements.

EU/UK Team

James Henderson

Counsel | London | jhenderson@Hunton.com

James is counsel in the firm's London office. He advises a broad range of clients on all areas of UK and EU data protection law, from general compliance issues and cross-border data transfers to cutting-edge technology issues, such as mobile apps, social media, online behavioral advertising, geolocation, and other technology, media, and telecommunications matters. James also has experience with IT law matters, including technology, software, and e-commerce and service agreements.

Anna Pateraki

Counsel | Brussels | apateraki@Hunton.com

Anna is counsel in the firm's Brussels office. Her practice is focused on all aspects of global and European data protection law, including global compliance programs, data transfers, privacy integrations, data breaches, Privacy Impact Assessments, and data processing agreements. She has extensive experience advising clients across a range of sectors on cutting-edge privacy issues, such as AI, online and mobile privacy, cloud computing, consumer programs, advertising, and life sciences.

Laura Léonard

Senior Attorney | Brussels | lleonard@Hunton.com

Laura is a senior attorney in the firm's Brussels office. She advises clients on myriad EU and Belgian data protection and privacy issues, including on the GDPR. She provides guidance to clients on a variety of privacy concerns related to emerging technologies across multiple industries, such as AI, connected devices, cybersecurity, cookies, and data analytics. She regularly assists clients on data breach issues, health data and regulatory compliance, international data transfers, and also with the drafting, review, and negotiation of data processing agreements.

Tiago Sérgio Cabral

Associate | Brussels | tcabral@Hunton.com

Tiago is an associate in the firm's Brussels office. He advises clients on a wide range of EU data protection and privacy issues. His experience includes advising clients on compliance with global privacy laws, cross-border data transfer strategies, cybersecurity incident response, and cutting-edge technologies. Tiago often drafts and reviews privacy policies, notices, and procedures.

Ashley Webber

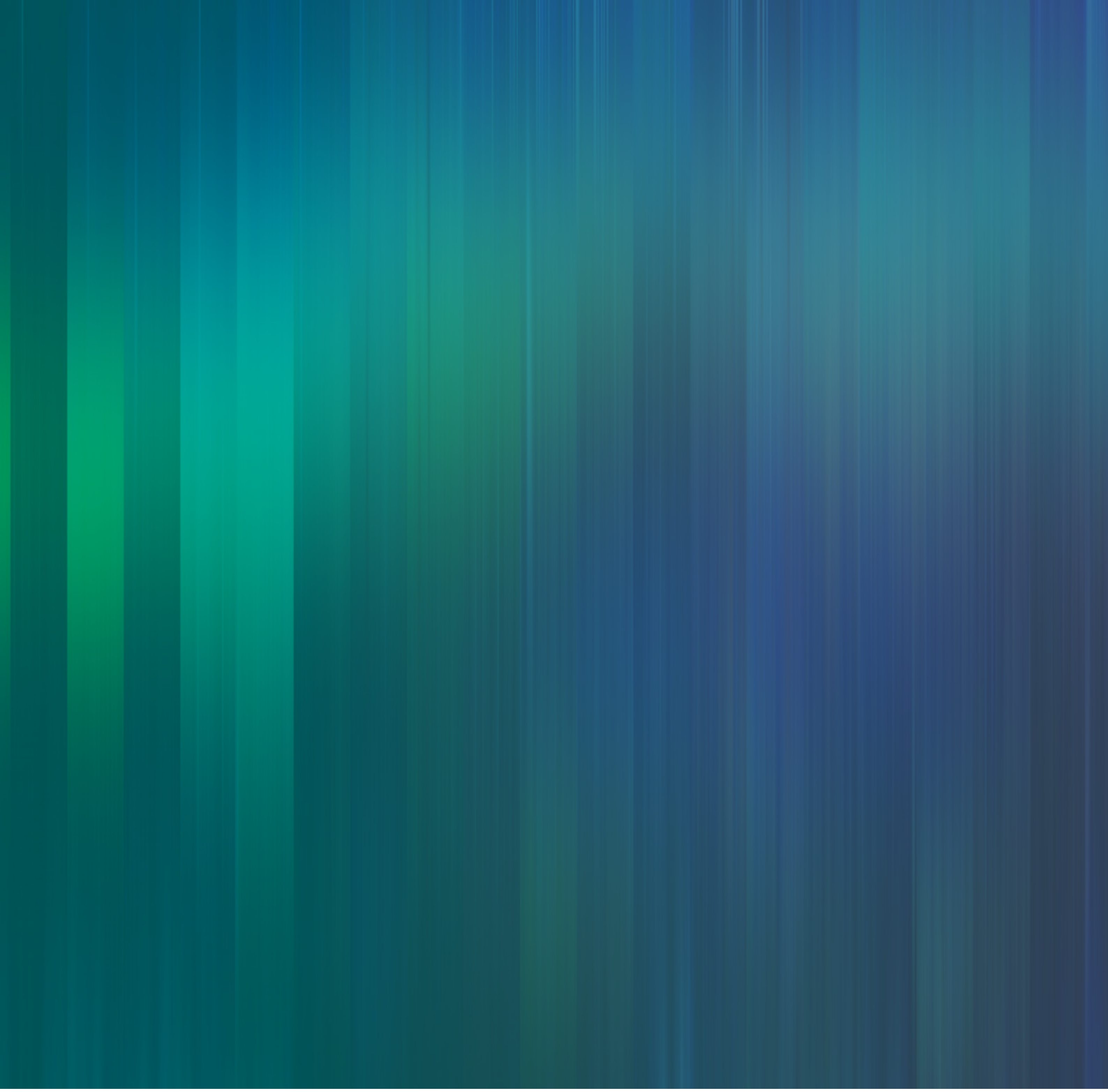
Associate | London | awebber@Hunton.com

Ashley is an associate in the firm's London office. She counsels clients on UK and EU data protection law, including the GDPR and AI Act. Her experience includes the use of data, cross-border data transfers, and drafting data processing agreements, privacy policies, and standards and processes. She also assists clients in managing global privacy compliance projects, identifying, and evaluating information security risks, and handling cybersecurity and data breach response.

Jonathan Wright

Associate | London | wrightj@Hunton.com

Jonathan is an associate in the firm's London office. He advises clients on all areas of UK and EU data protection law, including GDPR, e-commerce, incident response, online privacy, and general compliance work. Jonathan is experienced in managing global compliance projects and drafting, advising, and negotiating a variety of commercial contracts.



HUNTON