



# EU Artificial Intelligence Act Deep Dive





1. Introduction	04
2. Scope of the AI Act	06
3. Single Purpose AI Systems are differentiated by the associated risk	08
4. Roles and Obligations according to the Risk Categories	17
5. General-Purpose AI follows a different risk categorization scheme	22
6. Regulatory Governance and Enforcement	24
7. The AI Act grants easements for “sandbox” testing facilities	26
8. Non-Compliance will come at a high price – significantly more so than GDPR	28
9. AI Act will come into force step-by step	30
10. Glossary	32
Authors	34

# 1. Introduction

One of the key political priorities of the EU Commission for the 2019–2024 term was creating “A Europe fit for the digital age.” This ambitious agenda has led to the tabling of over 10 significant digital regulations, addressing areas such as the data economy, cybersecurity, and platform regulation. The AI Act is a crucial puzzle piece within this complex framework of EU digital regulation, which is striving to establish a comprehensive framework that addresses the complexities and potential risks associated with AI systems. While the following article focuses on the AI Act, it should always be viewed within the broader context of the entire EU digital regulatory landscape.

The AI Act introduces a framework aimed at regulating the deployment and usage of AI within the EU. It establishes a standardized process for single-purpose AI (SPAI) systems’ market entry and operational activation ensuring a cohesive approach across EU Member States. The AI Act, a product safety regulation, adopts a risk-based approach by categorizing AI systems based on their use case, thereby establishing compliance requirements according to the level of risk they pose to users. This includes the introduction of bans on certain AI applications deemed unethical or harmful, along with detailed requirements for AI applications considered high-risk to manage potential threats effectively. Further, it outlines transparent guidelines for AI technologies designated with limited risk. With the risk-based approach, AI ethics are the heart of the AI Act. Its focus on princi-

ples aims to leave the Act adaptable to as yet unknown iterations of AI technologies. However, the public use of general-purpose AI technology prompted the legislator to differentiate between single-purpose AI and general-purpose AI. The AI Act regulates the market entry for general-purpose AI models, regardless of the risk-based categorization of use cases, setting forth comprehensive rules for market oversight, governance, and enforcement to maintain integrity and public trust in AI innovations.

Given its abstract nature, the legislation contains areas that are yet to be fully defined. These are expected to be elaborated on through delegated and implementing acts, guidelines by the EU institutions, as well as harmonized standards developed by European Standardization Organizations. As a result, businesses can expect to receive more detailed guidance in the near future.

The AI Act is being published in the Official Journal of the European Union in June or July 2024, with its entry into force 20 days thereafter. This will mark the beginning of a phased implementation process to put the various rules and obligations of the AI Act into practice. For businesses, this means there is now a critical window to prepare for compliance.







## 2. Scope of the AI Act

In this chapter, we look at the legal scope of the AI Act and the technology defined as AI according to the regulation. For entities in the public sector and businesses across the EU, understanding these aspects is crucial for ensuring compliance and fostering AI innovations that respect ethical standards and societal values.

### 2.1 Definition of AI

The EU aimed for a clear definition of AI systems, aligning closely with the work of international bodies like the OECD. This approach seeks to ensure legal certainty and facilitate international convergence and acceptance.

An AI system, as defined in the AI Act, is a type of technology designed to make predictions, content suggestions, or decisions that can impact both physical and virtual environments. It achieves this by using various techniques, including machine learning, whereby it learns from data, and logic-based methods, which follow specific rules or knowledge structures. These systems can have different levels of autonomy and might operate on their own or as part of another product, either integrated into it or functioning separately. The adaptability of an AI system refers to its self-learning ability to change its behavior during use.

Furthermore, the recitals – which clarify the AI Act's regulatory text – specify that the definition of AI does not include basic traditional software or purely rule-based programming created by humans for automatic operations. Despite this, the definition remains wide, covering the majority of systems available on the market.

Finally, the Commission has been tasked with developing guidelines for applying the definition of an AI system, which grant further guidance of the defining aspects of AI under this regulation.

#### Definition of AI in the AI Act

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

## 2.2 The AI Act is an extra-territorial product safety regulation

The AI Act affects all AI system operators (see chapter 10), including private and public organizations of all sizes and sectors that offer AI products or services on the EU market. The primary objective of the AI Act is to promote the uptake of trustworthy AI while ensuring a high level of protection of

health, safety and fundamental rights of EU citizens. Moreover, it extends its jurisdiction to non-EU companies entering European markets with AI products. While there are no exemptions for smaller companies, the AI Act acknowledges the unique challenges faced by SMEs. Figure 1 explores the entities affected as well as use cases that are out of scope of the AI Act.

**Fig. 1 – Scope of Application**



### 1. Applicability

#### The AI Act applies to

- Providers (see chapter 4.1) introducing AI systems in the EU market, regardless of their geographic location.
- Providers and deployers of AI systems outside the EU, if the AI system's output is used within the EU.
- Deployers (see chapter 4.1) of AI systems within the EU.
- Importers and distributors of AI systems in the EU market.
- Manufacturers placing products with embedded AI systems on the EU market under their trademark.



### 2. Extraterritorial Reach

- The Act affects any business or organization that offers AI systems impacting individuals within the EU, irrespective of the organization's location.
- Public sector bodies and international organizations are out of scope if located outside the EU.



### 3. Exemptions

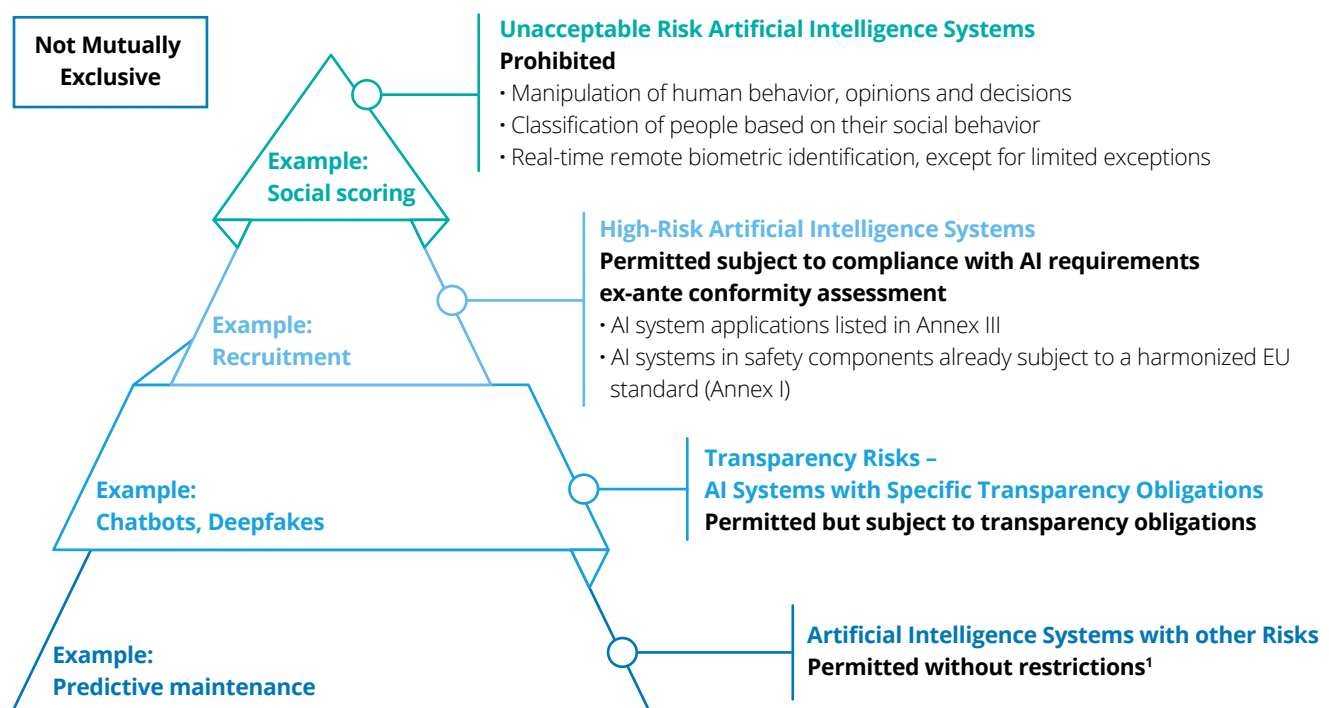
#### Certain use cases as well as entities are not covered by the Act:

- Activities involving the research and development of AI systems before they are released for commercial use or operational deployment.
- Free and open-source software is generally not subject to regulation unless it is categorized as unacceptable or high-risk AI application or a high-impact GPAI model.
- AI systems used for military or defense purposes.
- AI systems designed exclusively for scientific investigation and discovery.
- AI systems that were put on the market before the applicability of the AI Act. They fall under the AI Act if they undergo substantial modification.
- AI Systems used in purely personal non-professional activity.

# 3. Single Purpose AI Systems are differentiated by the associated risk

The AI Act focuses on how AI is used rather than the technology itself, employing a risk-based framework. This means obligations intensify with the user risk level. The Act identifies four specific risk categories, each with its corresponding set of requirements: unacceptable risk, high-risk, transparency risk and other risk. Companies are expected to undergo a process of assessing how the application of their AI systems falls into the four risk categories as shown in figure 2.

Fig. 2 – AI Act risk levels, with four layers of obligations for entities












### 3.1 Certain applications which severely impact the rights of individuals are outright banned

Recognizing the advantages of AI, policy-makers balanced its possibilities with the core of EU principles being aware that some AI applications might threaten funda-

mental values such as human dignity, freedom, equality, democracy, data privacy, and the rule of law: To safeguard these fundamental values, the AI Act prohibits specific AI applications. The ban on such systems will begin after a 6-month grace period following the AI Act's entry into force.

**Tab. 1 – Prohibited AI Applications**

Categories	Use Cases
 <b>AI-enabled manipulative techniques</b>	<p>Persuasion to engage in unwanted behaviours, nudging for subversion and impairment of autonomy, decision-making and free choices causing or reasonably likely to cause harm</p> <p>Excluding: common and legitimate commercial practices, e.g., advertising</p>
 <b>Biometric categorisation</b>	<p>Use of individual biometric data as face or fingerprint, to deduce or infer political opinion, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation</p> <p>Excluding: labelling, filtering or categorisation of biometric datasets</p>
 <b>Social scoring</b>	<p>Valuation or classification of natural persons or groups based on multiple data points related to social behaviour and leading to negative treatment</p> <p>Excluding: lawful evaluation practices of natural persons done for a specific purpose in compliance with national and Union law</p>
 <b>Real-time remote biometric identification</b>	<p>In publicly accessible spaces for the purpose of law enforcement</p> <p>Excluding the exceptions mentioned in Annex II</p>
 <b>Risk assessments of natural persons</b>	<p>Assessing persons traits and characteristics to predict the risk of committing a criminal offence</p> <p>Unless assessing involvement of a person objectively and verifiably linked to a crime</p>
 <b>Facial recognition databases based on untargeted scraping of facial images</b>	<p>Creation or expansion of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage</p>
 <b>Identifying emotions in workplace and education</b>	<p>Identifying or inferring emotions or intentions of natural persons on the basis of their biometric data related to places of work and education institutions</p> <p>Excluding: medical reasons such as therapy and safety reasons such as pilot tiredness assessment</p>

### 3.2 The focus of the AI Act is squarely set on “High-Risk AI Systems”

#### 3.2.1 Identifying High-Risk AI System

The core focus of the AI Act revolves around high-risk AI systems, as most obligations and protective measures outlined in this act refer to high-risk AI applications. High-risk AI systems are those that are deemed to negatively impact safety or fundamental rights of EU citizens and given that presumed risk need to be assessed before being put on the market and also throughout their life-cycle.

There are two potential pathways for AI systems to be designated as high-risk under the AI Act. The first one involves inclusion in the specific applications listed in Annex III

of the AI Act, while the second one pertains to products mentioned in Annex I. In either scenario, the entity using the AI will have the responsibility to self-determine whether its products or AI systems fall within these defined categories. Given the highly individual nature and rapid evolution of AI systems, these detailed assessments will likely occur on a case-by-case basis.

Notably, the list of high-risk applications may be subject to extensions and frequent updates. For example, the EU Commission retains the right to include new AI applications on the list of high-risk AI applications whenever those are deemed to pose a risk to health, safety, or fundamental rights of EU citizens.

“The EU AI Act represents an important step forward in the governance of artificial intelligence, offering organizations a clear framework for deploying AI systems responsibly. Ensuring compliance and mitigating risks involves conducting thorough assessments of AI risk classifications, maintaining a comprehensive inventory of AI assets, and clearly defining the roles and responsibilities of each operator. By following existing structures for managing compliance and security risks, organizations can navigate this new regulatory landscape with a robust governance framework and a proactive approach to risk management.”

#### Is all high-risk really high-risk?

To ensure that only AI presenting a demonstrably elevated risk is classified as high-risk, the EU has introduced opt-out exceptions for providers of certain AI systems in high-risk fields. AI systems that at first glance fall into the high-risk category but do not pose significant risks to health, safety, or fundamental rights may, under justifications, be excluded from the high-risk AI category. Consequently, they are not obliged to fulfill all associated obligations. This exemption applies to:

- The AI system is designed for a specific, narrow procedural task.
- The AI system's purpose is to enhance the outcome of a human activity that has already been completed.
- The AI system is designed to identify decision-making patterns and deviations but should not replace or influence prior human assessments without appropriate human review.
- The AI system is designed for preparatory tasks related to assessments outlined in the high-risk AI use cases listed in the law.









However, AI that is profiling will always be considered high-risk. In order to opt-out operators have to provide documentation and register in advance.

### 3.2.2 High-Risk Applications according to Annex III

The AI Act designates specific contexts outlined in Annex III in which AI applications are more likely to pose heightened risks to consumers. Any application falling within Annex III categories that potentially threaten health, safety, fundamental rights, the environment, democracy, or the rule of law is automati-

cally considered high-risk. Consequently, the algorithms and decision-making processes of these AI systems demand robust protections to mitigate potential harm, unless they fall within one of the exceptions mentioned in (see chapter 3.2.1 textbox on exception assessment). The rules for high-risk applications according to Annex III will apply 24 months after entry into force.

**Tab. 2 – High-Risk AI Applications Annex III**









Categories		Use Cases
	<b>Biometrics</b>	Remote biometric identification systems but only with prior authorization for exceptional circumstances listed in Annex II; also biometric categorisation and usage for emotion recognition
	<b>Critical infrastructure defined as in CER Directive</b>	Safety components in the management & operation of critical digital infrastructure (e.g., road traffic, supply of water/gas/heating/electricity)
	<b>Education and vocational training</b>	Admission to institutions at all levels as well as assessment of received educational level; also AI use for evaluation & steering of learning outcomes or monitoring & detection of prohibited behavior during tests
	<b>Employment, workers management and self-employment</b>	Used for recruitment for instance analysis & filtering of job applications or evaluation of candidates; also deciding on promotions, termination of work-related contractual relationships or allocation of tasks; used to monitor & evaluate the performance & behavior of a worker
	<b>Essential public &amp; private services</b>	Evaluation of eligibility for essential public assistance benefits & services; risk assessment & pricing in case of life & health insurance; evaluation of creditworthiness or establishment of credit score; evaluation & classification of emergency calls as well as establishment of emergency priorities
	<b>Law enforcement</b>	Used in polygraphs or to assess risk to become a victim of criminal offences; evaluation of evidence reliability & prosecution of criminal offences; profiling during detection, investigation & prosecution of criminal offences; risk assessment of (re-) offending based on profiling and assessment of behavioral & criminal traits
	<b>Migration, asylum and border control management</b>	Used in polygraphs or assessment of security risks; also if used for examination of asylum, visa & residence permits applications or detection, recognition & identification of individuals
	<b>Administration of justice and democratic processes</b>	Research and interpretation of facts & law; application of law; influence of voting behavior & outcome

### 3.2.3 AI systems that are Safety Components classify as High-Risk

The AI Act places particular emphasis on AI-embedded safety products and the associated potential risks. The Act specifies in Annex I sectors that are considered high-risk due to their importance for the health and safety of persons when AI is used in safety components. Operators in

these sectors must clarify whether an AI regulated by the Act is integrated into a product, constituting a safety component, and whether it is subject to third-party conformity assessment. The rules for high-risk applications according to Annex I will apply 36 months after entry into force. The AI Act regulates the following areas:







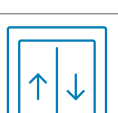



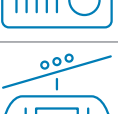
**Tab. 3 – High-Risk AI Applications Annex I**

Categories	Use Cases
 <b>Civil aviation<sup>2</sup></b>	All airports or parts of airports that are not exclusively used for military purposes as well as all operators, including air carriers, providing services at airports or parts of airports that are not exclusively used for military purposes <sup>3</sup>
 <b>Agricultural and forestry vehicles<sup>2</sup></b>	Tractors as well as trailers and interchangeable towed equipment <sup>3</sup>
 <b>Two-, three-wheel vehicles and quadricycles</b>	All two- or three-wheel vehicles and quadricycles
 <b>Marine equipment<sup>2</sup></b>	Equipment placed or to be placed on board of EU ships
 <b>Personal protection</b>	Personal protective equipment designed and manufactured to be worn or held by a person for protection against one or more risks to that person's health or safety, as well as some interchangeable components and connection systems for the equipment
 <b>Appliances burning gaseous fuels</b>	Appliances burning gaseous fuels used for, amongst others, cooking, refrigeration, air-conditioning, space heating, hot water production, lighting or washing; also, all fittings that are safety devices or controlling devices incorporated into an appliance
 <b>Rail system<sup>2</sup></b>	Rail system including vehicles, infrastructure, energy and signaling systems <sup>3</sup>
 <b>Motor vehicles and trailers; systems, components and separate technical units intended for such vehicles<sup>2</sup></b>	Motor vehicles and their trailers; including autonomous driving <sup>3</sup>

<sup>2</sup> The sectors mentioned in Section B are subject to specific articles of the EU AI Act and may experience differences in application.

<sup>3</sup> Amongst others.



	<b>Civil aviation, European air space, aerodomes<sup>2</sup></b>	The design and production of products, parts and equipment to control aircraft remotely by a natural or legal person, as well as the design, production, maintenance and operation of aircrafts <sup>3</sup>
	<b>Medical devices</b>	Medical devices for human use and accessories for such devices as well as clinical investigations concerning such medical devices and accessories <sup>3</sup>
	<b>In vitro diagnostic medical devices</b>	In vitro diagnostic medical devices for human use and accessories for such devices <sup>3</sup>
	<b>Machinery</b>	Machinery, interchangeable equipments and lifting accessories (e.g., robots) <sup>3</sup>
	<b>Toys</b>	Products designed or intended for use in play by children under 14 years of age (e.g., connected toys and IoT devices)
	<b>Recreational craft and personal watercraft</b>	Recreational craft as well as propulsion engines installed on watercraft <sup>3</sup>
	<b>Lifts</b>	Lifts permanently serving buildings and constructions for mainly the transport of persons with or without goods
	<b>Equipment and protective systems intended for use in potentially explosive atmospheres</b>	Equipment and protective systems intended for use in potentially explosive atmospheres as well as components incorporated within the equipment or protective system <sup>3</sup>
	<b>Pressure equipment</b>	The design, manufacture and conformity assessment of pressure equipment and assemblies
	<b>Radio equipment</b>	Any kind of radio equipment that is anything connected via radio waves (e.g., WiFi, Bluetooth, 5G in laptops, phones, IoT devices)
	<b>Cableway installations</b>	New cableway installations designed to transport persons, to modifications of cableway installations requiring a new authorization, and to subsystems and safety components for cableway installations

### 3.3 Rules for Transparency and Other Risks

For AI applications with limited risk to individuals, the main requirement is to follow certain rules on transparency. However, while some AI systems may only need to adhere to transparency obligations, it is important to note that AI systems in other risk categories are also required to comply with these transparency rules in addition to their specific regulatory requirements. An example for a limited risk AI system is AI-based chatbots which require explicit notification before use, ensuring users are aware that their interaction is with a machine and granting them the option to be redirected to human assistance.

Other risk AI systems do not have any obligations under the AI Act. This classification could encompass a considerable portion of existing AI applications across various sectors, including spam filters, AI-enabled video games, and inventory management systems. All operators can comply volun-

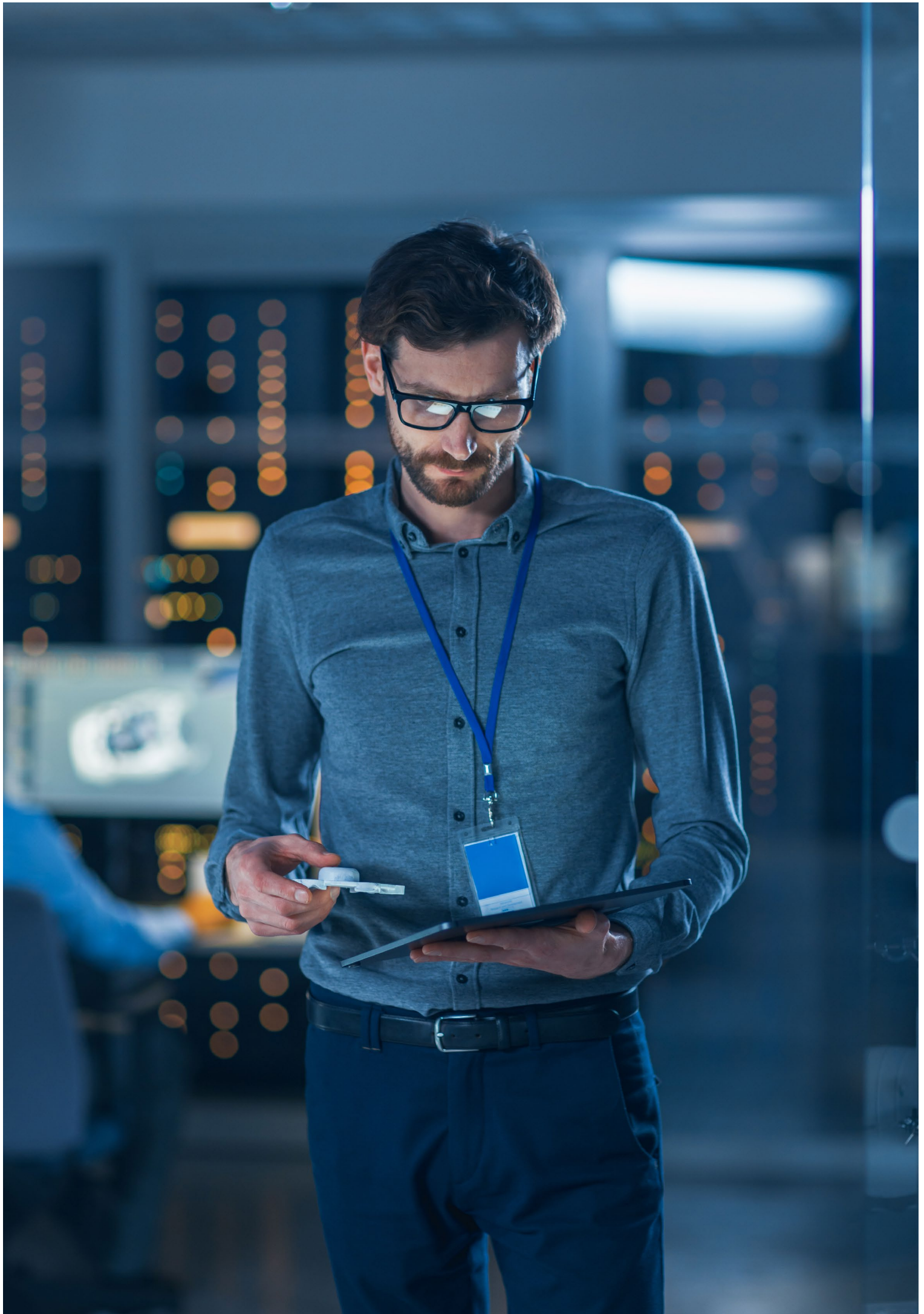
tarily with code-of-conduct in accordance with ethical and trustworthy AI standards in the union. The AI Office (see chapter 6) will support and promote the development of such codes of conduct, considering existing technical solutions and industry best practices.

It is important to bear in mind that AI systems with no obligations under the AI Act may still pose business and security risks, as well as regulatory obligations under other EU laws, that should not be disregarded.











# 4. Roles and Obligations according to the Risk Categories

## 4.1 Providers, deployers, distributors and importers are accountable

The responsibilities outlined in the AI Act vary significantly based on the specific circumstances of each AI operator (see chapter 10). The rules and obligations can differ depending on the type of role and use case involved. Moreover, while the AI Act outlines the obligations, these will be further specified in the coming years through delegated and implementing acts of the Commission, as well as harmonized standards and work of other working groups.

Consequently, it is essential for each operator to identify their relevant risk category. The AI Act organizes operators into four principal categories: provider, deployer, distributor, and importer. Each category is held to distinct obligations under the AI Act and is defined as follows:

Fig. 3 – Definition of Roles



### Special case for providers:

If any of the following scenarios occurs, any operator (such as a distributor or deployer) may transition into a "provider" and, consequently, be obligated to fulfill the responsibilities associated with high-risk AI and general-purpose AI as a provider:

1. If they associate their name or trademark with a high-risk AI system that has already been introduced to the market or put into service. However, contractual exemptions can be applied.
2. If they make substantial modifications to a high-risk AI system that has already been placed on the market, and it continues to pose a high risk in its new use.
3. If they alter the intended purpose of an AI system or general-purpose AI that was not originally classified as high-risk AI but becomes high-risk AI due to the new modifications.

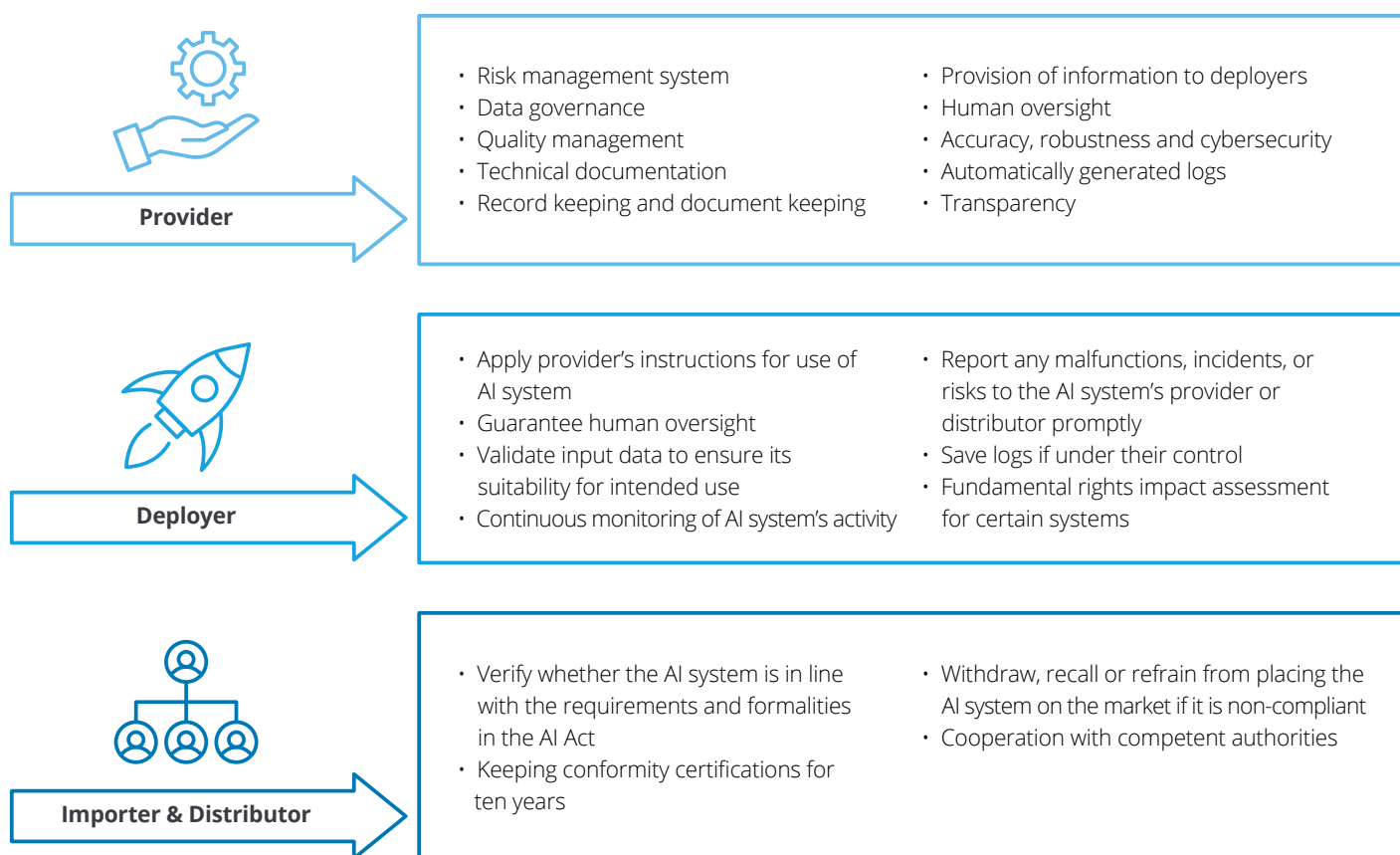
## 4.2 Distinct responsibilities depending on the role of each stakeholder

The following illustration offers a preview of the obligations and tasks that different operators will be required to implement. Each obligation is delineated more comprehensively in the final legal text and may also undergo further detailing. Generally speaking, there is an obligation of mutual recognition between the Member States, so that the assessment done by one national authority has to be recognized by the other. However, each Member State may act upon potential violations.

Providers and deployers of all AI systems must ensure adequate AI literacy among their staff and relevant individuals, considering their technical expertise, experience, education, training, and the intended use of the AI systems, as well as the affected persons or groups. The AI Act emphasizes the importance of AI literacy, aiming to furnish AI System

operators with the necessary knowledge and resources to make well-informed decisions about AI systems. This not only involves understanding the accurate application of technical elements during the development phase of AI systems but also extends to knowing the right measures to apply during its use and correct interpretation and usage of the output.

**Fig. 4 – High-level Overview/Summary of Obligations of High Risk AI Systems**



One of the main obligations for providers of high-risk AI systems is setting up a Risk Management System (RMS) around the respective system which is covering all phases of an AI system's lifecycle. According to the AI Act, the following steps should be ensured:

- **Safety by design**

Elimination or reduction of risks identified and evaluated pursuant to paragraph 2 in as far as technically feasible through adequate design and development of the high-risk AI system

- **Protective measures**

Where appropriate, implementation of adequate mitigation and control measures addressing risks that cannot be eliminated

- **Information for safety**

Provision of information required pursuant to Article 13 (Transparency and provision of information to deployers) and, where appropriate, training to deployers

Another important requirement is setting up a Quality Management System which shall also encompass the AI system's entire lifecycle with regard to the following factors:

- 1. Pre-Market Phase**

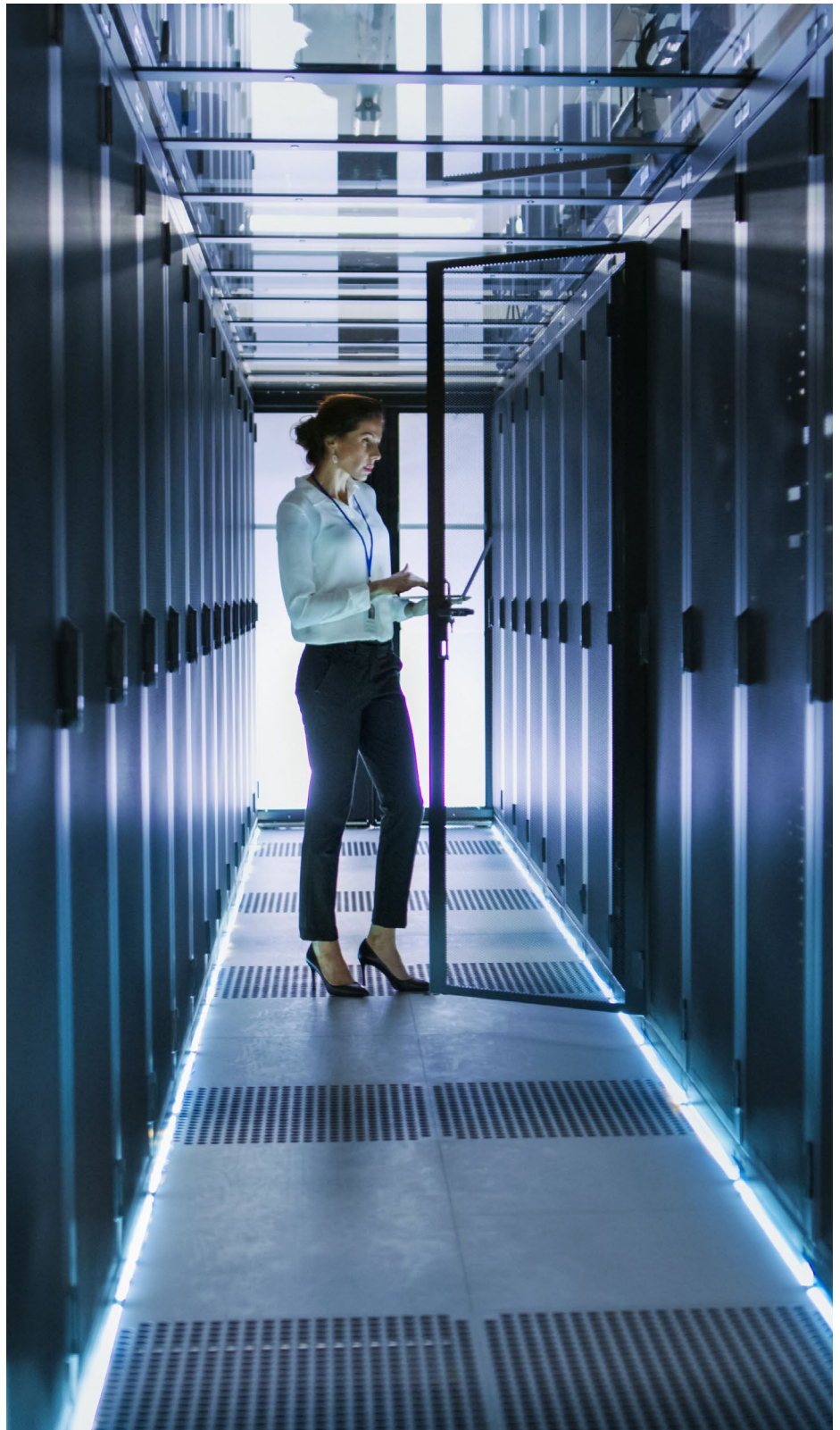
This includes a strategy for regulatory compliance, design control and verification, system examination, testing and validation of AI systems, and technical specification.

- 2. Post-Market Phase**

Quality control, reporting of serious incidents, and a post-market monitoring system are all required.

- 3. Continuous Phase**

This involves data management systems and procedures, RMS, communication with authorities, and document and record-keeping, including logging. Resource management, including security of supply, and an accountability framework are also included.



4.3 Two Types of Conformity Assessment under the AI Act

The European Union (EU) has established a New Legislative Framework (NLF) that certain products must be evaluated under before they can be sold in the market. This framework ensures that these products meet specific EU regulations and standards for safety, quality, and performance. As part of the NLF, the AI Act requires “conformity assessments” followed by a “declaration of conformity” as prerequisites for products to enter the market and demonstrate compliance with the respective obligations.

Under the EU AI Act, the conformity assessments for high-risk AI systems can be conducted by the providers themselves or with the support of third parties. For all high-risk AI applications listed in Annex III (e.g., employment, essential public and private services), providers may conduct a self-assessment based internal controls and issue the declaration of conformity.

All AI systems listed in Annex I (e.g., aviation, automotive, and medical devices) must seek support from third parties. In this case, the conformity assessment must be performed by an accredited “notified body” suitable for the type of AI system being inspected. Notified bodies are conformity assessment bodies that have been notified by the notifying authority. If the AI system is deemed compliant by the notified body, the provider must issue a declaration of conformity.

Only providers of high-risk biometric systems have the option to conduct internal controls or opt for third-party assessment.

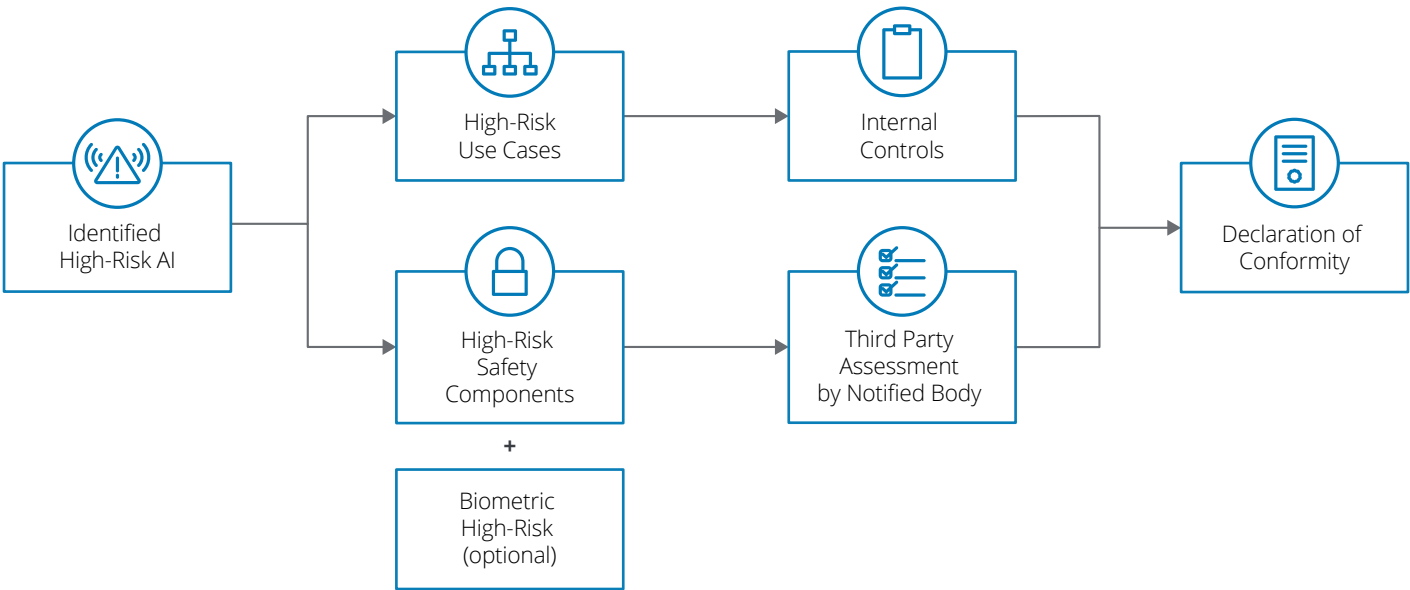
Providers who self-assess are presumed compliant if they adhere to harmonized standards. The Commission issued the standardization requests, which will include reporting and documentation deliverables to enhance AI system resource efficiency. These harmonized standards are expected before the application of the respective rules and are already in development, with CEN (European Committee for Standardi-

zation) and CENELEC (European Committee for Electrotechnical Standardization) leading the process. Providers of high-risk AI systems may benefit from a presumption of compliance with data and data governance obligations if the data used for training their AI systems accurately reflects the specific geographical, behavioral, contextual, or functional settings in which the systems are intended to be used. Under these conditions, providers are generally considered compliant with the obligations mentioned in Article 10, meaning they would not need to undergo the usual rigorous processes of validating and testing data sets for biases and unrepresentative training data.

Additionally, providers who have received a certificate or statement of conformity under a cybersecurity scheme pursuant to the EU Cybersecurity Act are presumed to be compliant with the cybersecurity obligations mentioned in Article 15.

All approved high-risk AI systems will be published in a EU-wide registry.

Fig. 5 – Third Party Assessment vs Internal Controls







#### 4.4 Distinctive Aspects of Fundamental Rights Impact Assessment for High-Risk AI Systems

Before deploying high-risk AI systems, bodies governed by public law, private operators providing public services, as well as those involved in evaluating credit-worthiness and risk assessment for life insurance policies must conduct a fundamental rights impact assessment. This involves describing the system's intended use, frequency of use, identifying affected individuals or groups, assessing potential risks, outlining human oversight measures,

and detailing risk mitigation strategies. Once completed, deployers must inform the market surveillance authority of the assessment results. If a data protection impact assessment has already been conducted, it should be integrated with the fundamental rights impact assessment. To aid deployers in fulfilling these obligations, the EU AI Office will develop a questionnaire template for simplified implementation. Member States may assign or establish institutions to oversee the protection of fundamental right as further explained in chapter 6.1.

# 5. General-Purpose AI follows a different risk categorization scheme

The regulation of general-purpose AI models, which are trained on vast datasets and capable of performing a wide array of tasks, proved to be the most contentious aspect of the AI Act negotiations.

The AI Act adopts a risk-based approach, with high-risk AI systems subject to more stringent requirements. However, the generality and versatility of general-purpose AI make precise risk categorization challenging, as the intended purpose of downstream systems or applications incorporating these systems is often unclear.

To address this issue, the final version of the AI Act introduces a dedicated regime in Chapter V for providers of general-purpose AI models ("foundation models"), rather than the general-purpose AI systems themselves. An AI model is a core component of an AI system, used to make inferences from inputs to produce outputs. Model parameters typically remain fixed after the build phase concludes, making the risks posed by general-purpose AI models easier to estimate and regulate compared to those of complete AI systems. As models and systems are treated separately, a general-purpose AI model itself will not be classified as a high-risk AI system. However, a general-purpose AI system built upon a general-purpose AI model may still fall into one of the established risk categories. For general-purpose AI models, the European policymakers agreed on a two-tiered approach, which consists of obligations for providers of general-purpose AI models with and

without systemic impact, i.e., models with high impact. A general-purpose AI model is classified as a high-impact model when it demonstrates a systemic risk through specific technical criteria. This is presumed if the cumulative compute power used during its training exceeds a certain threshold, currently set at  $10^{25}$  floating point operations (FLOPs). Alternatively, the Commission may classify it as such if advised by a scientific panel alert, indicating its potential for significant impacts. They use the assessment criteria listed in Annex XIII which may be adjusted over time to keep pace with technological advancements through delegated acts adopted by the Commission. Providers of general-purpose AI models must adhere to certain standards. To facilitate compliance, the AI Office, in collaboration with relevant stakeholders such as civil society organizations, industry representatives, academia, downstream providers, and independent experts, will encourage and support the development of additional Union-level codes of practice. These codes of practice are voluntary for all companies using general-purpose AI but grant a presumption of conformity to anyone who applies them. The AI Office is tasked with drawing up these codes of practice, monitoring and evaluating them, and being the future recipient of implementation reports.

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, whose parameters are publicly available, and which are not considered systemic risk, will have only limited obligations.

**General-Purpose AI model** means an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications.

**General-Purpose AI System** means an AI application which is based on an underlying general-purpose AI model. This application has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems.

**Tab. 4 – Obligations of General-Purpose AI Models**

General-Purpose AI Models	High-Impact General-Purpose AI Models (“systemic risk”)
<p>Large models and systems capable of competently performing a wide range of distinctive tasks, such as generating video, text, images or computer code, or conversing</p> <ul style="list-style-type: none"> <li>• Drawing up and keeping up-to-date technical documentation for the AI Office and national authorities (as listed in Annex XI) and downstream providers (as listed in Annex XII)</li> <li>• Protecting intellectual property rights, trade secrets and confidential business information</li> <li>• Enabling understanding about the limitations and capabilities of the GPAI models</li> <li>• Complying with EU copyright law and disseminating detailed summaries about the content used in training</li> </ul>	<p>Foundation models trained with large amount of data and with advanced complexity, capabilities, and performance well above the average, which can disseminate systemic risks along the value chain</p> <ul style="list-style-type: none"> <li>• Complying with all requirements applicable to all general-purpose AI models and systems</li> <li>• Conducting model evaluations</li> <li>• Assessing and mitigating systemic risks including their sources</li> <li>• Conducting adversarial testing</li> <li>• Keeping track of, documenting and reporting of serious incidents to the EU Commission</li> <li>• Ensuring sufficient cybersecurity protection</li> <li>• Reporting on energy efficiency and estimate energy consumption for training</li> </ul>

Providers of free and open source GPAI models only have to provide detailed summary about the content used for training and abide with EU copyright laws. If deemed as a GPAI model with systemic risk all obligations apply.

# 6. Regulatory Governance and Enforcement

The competences of the enforcement of the AI Act will be distributed between the newly established AI Office in the European Commission and supervisory authorities in the Member States.

Both the EU Commission and Member States have distinct responsibilities and work together to monitor and enforce the new rules for AI systems and general-purpose AI models. Whereas the EU Commission is mainly responsible for supervision of general-purpose AI models, the Member States' authorities are responsible for enforcing the AI systems' risk-based rules as well as coordinating the sandboxes on Member State level. The following chapter provides insights on the specific responsibilities, the governance structure and the interplay of EU Commission and Member States.

## 6.1 National Level – Member State Enforcement

The Member States create the market surveillance authority (agency level). The market surveillance authority is primarily tasked with enforcing the AI Act at national level.

The market surveillance authorities are responsible for ensuring that AI systems adhere to the prescribed standards and regulations. For example, the market surveillance authority will oversee the correctness of the conformity assessment conducted by high-risk AI providers. In the course of investigations, market surveillance authorities may take necessary actions such as accessing documentation as well as the training, validation and testing data sets used for the development of high-risk AI systems and accessing the source code of high-risk AI. Providers of high-risk AI are obliged to cooperate with the authorities.

The notifying authority will also be responsible for assigning the conformity assessment bodies which upon proper notification can qualify as notified bodies (see chapter 4). The notified bodies must comply with several conditions to qualify as one. Such obligations include being established as a legal person under national law, fulfilling organizational requirements to fulfill their tasks and being independent from the high-risk AI providers.

Additionally, each Member State will have to assign specific responsibilities and authorities to existing or newly established bodies dedicated to protecting fundamental rights concerning AI. These bodies must operate independently and impartially, ensuring that companies adhere to fundamental rights principles in AI development, deployment, and use.

## 6.2 European Level – EU Enforcement

To streamline and oversee the implementation of the Act, the EU set up the EU AI Office in February 2023, a new entity established by the EU Commission. It has a key role in the implementation of the AI Act. The AI Office is established as a Commission service embedded in DG CONNECT and thus holds more freedoms in its decision-making process and can act in a more dynamic manner. It will be composed of five main departments. Each department will be led by a director responsible for overseeing the implementation of the AI Act. The AI Office shall employ a total of 140 people, including technological experts, lawyers, and policy specialists. Currently, it has over 50 tasks

open related to implementing the AI Act. The AI Act mentions a variety of aspects that shall be subject to further implementation by the AI Office through delegated and implementing acts. As the AI Act was kept intentionally on an abstract level, it is highly dependent on further clarification.

While delegated acts relate mostly to the amendments to the legislative text, implementing acts are measures of individual application. For instance, the AI Office may modify the list of each Annex of the AI Act by means of a delegated Act. A particular task, given the implementation timeline, is the establishment of concrete examples that constitute prohibited AI or specifically do not constitute prohibited AI. These steps aim to ensure the effective implementation of the AI Act and to specify the rules and concepts stipulated in the AI Act.

Moreover, the EU AI Office will be responsible for enforcing the AI Act obligations for general-purpose AI models. In this context, it will develop design tools, methodologies, and benchmarks to evaluate the capabilities and reach of general-purpose AI models and identify models with systemic risks in concert with academia and industry stakeholders. Last but not least, the EU AI Office will host a public registry listing all high-risk AI applications which entered the market.

Next to the AI Office, there are two more EU bodies that will also influence the enforcement of the AI Act. First, to enhance collaboration and ensure comprehensive guidance on AI regulation, the Advisory



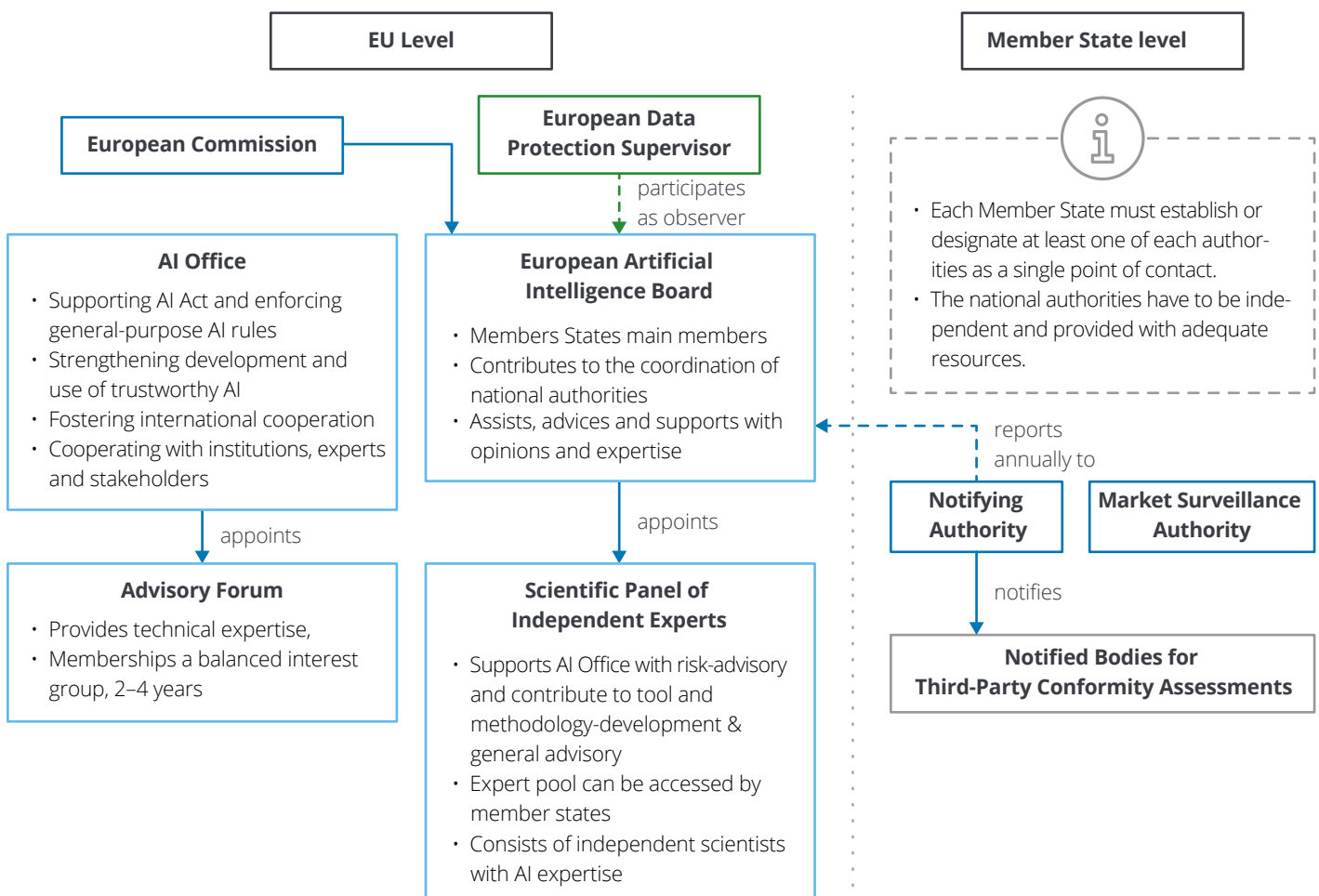
Forum will be responsible. This forum comprises a diverse array of stakeholders, including industry experts, civil society representatives, academic scholars, and governmental officials. Appointed by the EU Commission, members of the Advisory Forum offer technical expertise and strategic insights to support the implementation of the AI Act. Secondly, the Scientific Panel of Independent Experts is responsible for advising and alerting the Commission on systemic risks of general-purpose AI.

### 6.3 Interplay of European and National enforcement

Comprised of representatives from each Member State, alongside observers such as the European Data Protection Supervisor and the AI Office, the European Artificial Intelligence Board collaborates with relevant stakeholders to ensure consistent and effective application of the regulation. Assigned with tasks ranging from coordinating national competent authorities to issuing recommendations on regulatory matters, the Board plays a critical role in

fostering cooperation, sharing expertise, and promoting a good understanding of AI across the EU. Moreover, to effectively address all relevant challenges surrounding the AI Act, the Board will be divided in different sub-committees, focusing on, for example, the alignment of sectorial or national legislation. One can expect the different notifying bodies and market surveillance authorities of each Member State to participate in the different sub-committees and representing their respective interests.

**Fig. 6 – Regulatory Governance Structure**



# 7. The AI Act grants easements for “sandbox” testing facilities

Member States are mandated to establish AI regulatory sandboxes at the national level within 24 months of the entry into force of the Regulation, which is expected in Q3 2026. Member States can, however, establish a joint sandbox or join an already established sandbox. Since the main objective is to give all EU-based companies the option to participate in a regulatory sandbox, equal access and equal coverage for the participating Member States must be provided. Additionally, Member States have the option to set up regional or local sandboxes. Hence, it is expected that bigger states may set up several sandboxes to ensure regional or local support for SMEs. Apart from that, the European Data Protection Supervisor may also establish an AI regulatory sandbox for the EU-level.

## 7.1 AI Regulatory Sandboxes

AI regulatory sandboxes are controlled environments where operators of AI systems can develop, train, test, and validate AI systems before market deployment. They offer a safe space for experimentation, allowing for the exploration of AI applications under the supervision of competent authorities. In the spirit of improving the EU's Innovative Initiative, regulatory sandboxes stand as pioneering project, facilitating the development and testing of AI systems within a controlled environment. Additionally, the national competent authorities have to allocate sufficient resources to comply with the requirements mentioned in the AI Act. Each sandbox will have to submit annual reports on the activities, such as best practices, incidents, lessons learned and the set-up of the sandbox to the EU AI Office.

Both, public and private entities can join – after application – the sandboxes to test their AI systems against the obligations of the AI Act. Entities joining the sandbox are guided, supervised and supported in identifying risks relating to fundamental rights, health and safety. Furthermore, each participating entity should be given an exit report detailing the activities carried out in the sandbox and the related results and learning outcomes. This exit report will function as a document to demonstrate compliance with the regulation through the conformity assessment (presumption of conformity) and hence may be a competitive advantage for participating companies.

The AI regulatory sandboxes serve as catalysts for innovation in the AI landscape, offering a structured and supportive environment for the development and testing of AI systems while ensuring compliance with regulatory standards. More importantly, the exit reports for successful participants of regulatory sandboxes serve as a presumption of conformity for the necessary conformity assessment of high-risk AI systems.

### 7.1.1 Real-world Testing of High-Risk AI Systems Outside of the Regulatory Sandbox

While regulatory sandboxes offer controlled environments for initial testing and validation, real-world testing complements these efforts by providing insights into real-world performance, usability, and user feedback, ultimately contributing to the responsible and effective deployment of AI technologies. Real-world testing of AI systems outside regulatory sandboxes offers providers the opportunity to test high-risk AI systems listed in Annex III. Such testing requires adherence to a detailed real-world testing plan approved by market surveillance authorities. Providers must ensure compliance with Union and national law, including ethical considerations. Testing can be conducted independently or in collaboration with prospective deployers, with informed consent from participants. Moreover, strict conditions govern testing duration, data protection, oversight, and reversibility of AI system decisions and any incidents must be reported promptly to market surveillance authorities. Before applying the AI system to individuals, an informed consent from subjects is essential, detailing the nature, objectives, duration, rights, and contact information for further inquiries. Finally, it is important to note that providers bear liability for damages arising from testing activities.

### 7.2 Measures Supporting SMEs and Start-ups to Meet Act Standards

The AI Act aims to simplify certain aspects of regulatory requirements for SMEs and start-ups. Member States are tasked with implementing measures to support SMEs and start-ups in navigating the regulatory landscape of AI. This includes granting them priority access to AI regulatory sandboxes, organizing tailored awareness-raising and training activities, establishing communication channels for advice and inquiries, as well as facilitating their participation in the standardization process.

Furthermore, penalties for breach of obligations shall be adjusted based on specific factors such as the size and market presence of SMEs and start-ups.

Additionally, the EU AI Office plays a role by providing standardized templates, maintaining an information platform, conducting awareness campaigns, and promoting best practices in public procurement procedures related to AI systems. These efforts aim to empower SMEs and start-ups to comply with regulations and thrive in the AI ecosystem.

# 8. Non-Compliance will come at a high price – significantly more so than GDPR

The AI Act's penalty regime is structured based on the nature of the violation, considering whether it involves unacceptable systems, high-risk AI or general-purpose AI models, with fines increasing according to the risk category. Simply put, the higher the risk category, the higher the fine.

Member States are responsible for establishing rules concerning penalties and ensuring their enforcement. For example, each Member State has the discretion to determine the use of warnings and other non-monetary measures, if any. Furthermore, they must consistently consider the particular interests of SMEs and start-ups. National authorities are also mandated to assess the nature, gravity, and duration of each infringement, as well as whether the entity in question is a repeat offender, when determining the amount of each fine.

The higher option applies, unless pertaining to SMEs or start-ups. In addition to monetary fines, national supervisors may forcibly remove non-compliant AI systems from the market.

**Fig. 7 – Fines for operators of AI Systems**



1. Up to 35 m. EUR or for companies 7% of the GAT, for non-compliance with the prohibitions



2. Up to 15 m. EUR or for companies 3% of the GAT, for infringements to obligations of high-risk AI



3. Up to 15 m. EUR or for companies 3% of the GAT, for infringements to obligations of general-purpose AI



4. Up to 7.5 m. EUR or for companies 1% of the GAT, for supplying incorrect, incomplete or misleading information







# 9. AI Act will come into force step-by step

Twenty days after being published in the Official Journal, the EU AI Act comes into force, marking the start of the official implementation period. However, not all obligations take effect simultaneously; some require immediate action, while others allow for a longer implementation period for operators to comply with the established requirements.

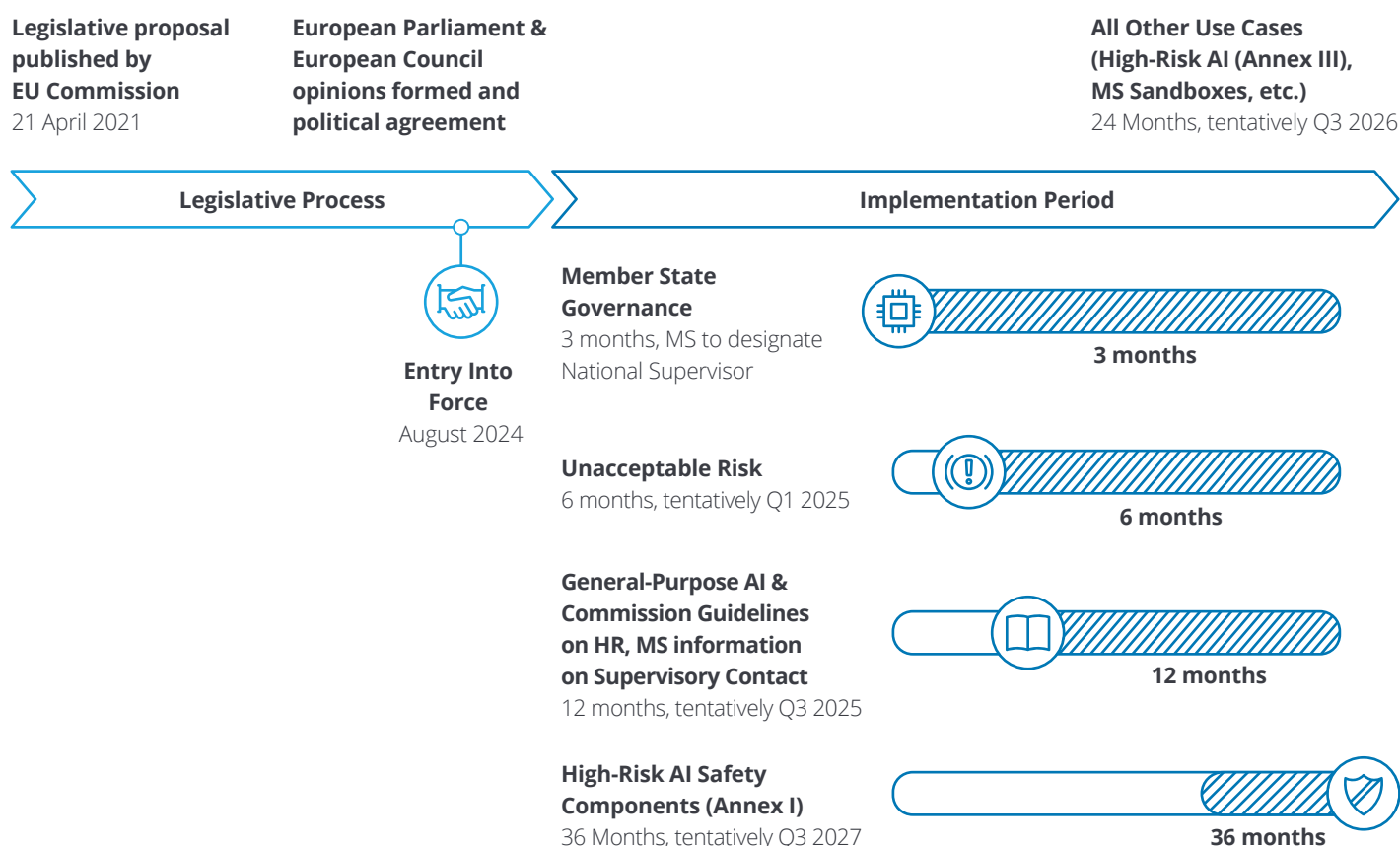
While most provisions will be implemented within the standard 24-month timeframe, some prohibitions and obligations will be enforced sooner, within 6 or 12 months

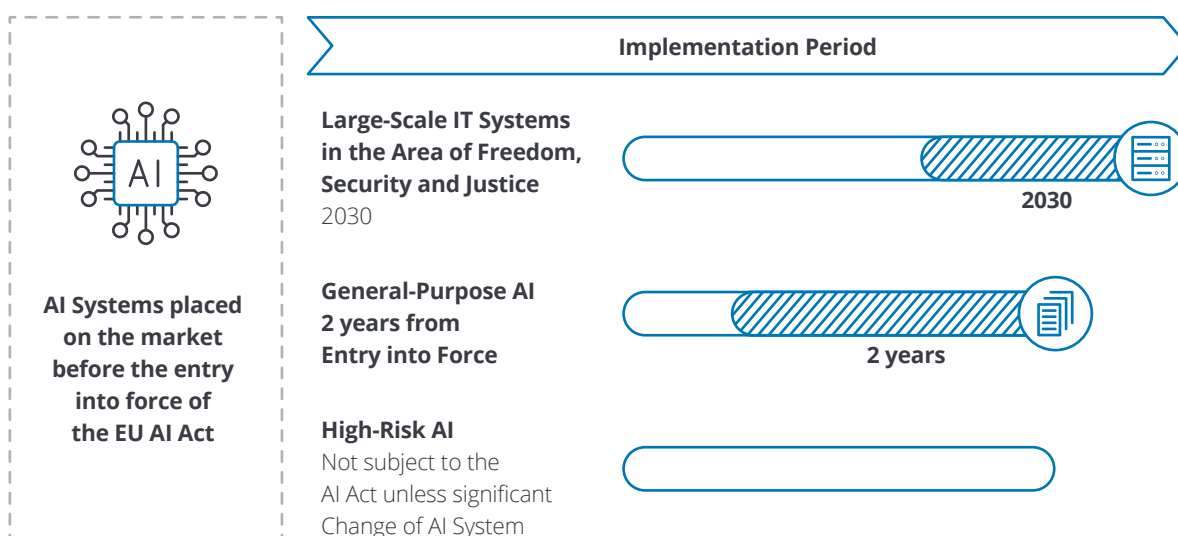
from the Act's entry into force. Others will have a longer implementation period of up to 36 months. The following illustration outlines key aspects that all operators in the EU market should keep in mind.

AI systems that were placed into the EU market before the entry into force of the AI Act or shortly after may not be directly affected by the EU AI Act or receive an extended implementation period, as stipulated in figure 9. Therefore, general-purpose AI that has entered the market before the

entry into force of the AI Act or within the first 12 months after the entry into force have 36 months to implement the requirements of the EU AI Act. And high-risk AI that entered the market before the entry into force or within the first 24 months after the entry into force is not automatically subject to the AI Act. Only upon significant changes done to the AI system, they will have to apply the rules of the AI Act, though it remains to be seen what qualifies as significant changes and how strict the Commission will apply this rule.

**Fig. 8 – Implementation Timeline AI Act**



**Fig. 9 – Implementation Timeline AI Act – Special Cases**

The European Commission has recently initiated the AI Pact. This initiative is designed to support businesses in voluntarily complying with the AI Act ahead of its legal enforcement in the second quarter of 2026. The AI Pact serves as a collaborative platform, allowing companies to exchange ideas and strategies for adhering to the AI Act's guidelines. Businesses are currently invited to show their interest in this pact, with a preliminary meeting for stakeholders scheduled for early to mid-2024. By participating, companies will pledge to conform to the AI Act and will detail their compliance efforts. These measures will be collected and made public by the Commission. The Commis-

sion's role includes helping companies understand the AI Act, aiding in their preparation and adjustment, promoting knowledge exchange, and fostering trust in AI technologies.

Furthermore, the CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization) have commenced the process of operationalizing the AI Act through standards. For companies applying or planning to apply AI systems, a proactive approach is essential to guarantee compliance by the expected deadline, entities should have an implementation plan and start as early as possible.

Even if not all the technical details have been clarified yet, the AI Act gives a sufficient impression of the scope and objective of the future regulation. Companies will have to adapt many internal processes and strengthen risk management systems. However, they can build on existing processes within the company and learn from measures from previous laws such as the GDPR. We recommend that companies start preparing now and sensitize their employees to the new law, take stock of their AI systems, ensure appropriate governance measures, install proper risk classification and risk management over AI and meticulously review AI systems classified as high-risk.

# 10. Glossary

## Wording taken from AI Act

**Provider:** A natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system, or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

**Downstream provider:** A provider of an AI system, including a general-purpose AI system, which integrates an AI model, regardless of whether the model is provided by themselves and vertically integrated or provided by another entity based on contractual relations.

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

**Authorized representative:** A natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.

**Importer:** A natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

**Distributor:** A natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

**Operator:** A provider, product manufacturer, deployer, authorized representative, importer or distributor.

**Biometric data:** Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, such as facial images or dactyloscopic data.

**Biometric identification:** The automated recognition of physical, physiological, behavioral, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database.

**Biometric verification:** The automated, one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data.

**Emotion recognition system:** An AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data.

**Biometric categorization system:** An AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons.

**Remote biometric identification system:** An AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database.

**Real-time remote biometric identification system:** A remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay and comprises not only instant identification, but also limited short delays in order to avoid circumvention.

**Deep fake:** AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful.

# Authors



**Dr. Till Contzen**

Partner | Legal  
Intangibles, Data & Technology  
(Head for Germany)  
Tel: +49 69 71918 8439  
tcontzen@deloitte.de



**David Thogmartin**

Partner | Risk Advisory  
aiStudio | AI & Data Analytics  
Tel: +49 211 8772 2336  
dthogmartin@deloitte.de



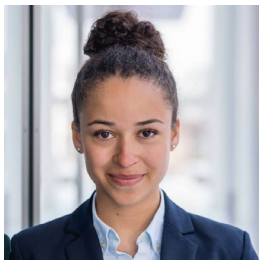
**Torsten Berge**

Director  
Algorithm & AI Assurance Lead DE  
Tel: +49 511 3023 4453  
tberge@deloitte.de



**Mosche Orth**

Manager  
Deloitte EU Policy Centre  
Tel: +49 511 3023 4167  
moorth@deloitte.de



**Zoe Marie Lohoff**

Algorithm Assurance  
Tel: +49 221 9732 4273  
zolohoff@deloitte.de







Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/de/UeberUns](http://www.deloitte.com/de/UeberUns) to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 457,000 people worldwide make an impact that matters at [www.deloitte.com/de](http://www.deloitte.com/de).

This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.