1

Companies that are beginning to know the Regulation

Guide 1. Introduction to the AI Act

European Artificial Intelligence Act

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

This guide has been developed within the framework of the development of the Spanish AI regulatory sandbox pilot, in collaboration between the participants, technical assistance, potential national competent authorities and the sandbox expert advisory group.

The guide aims to serve as an introductory support to the European Regulation on Artificial Intelligence and their applicable obligations. Although **it is not binding and does not replace or develop the applicable regulations, it provides practical recommendations** aligned with regulatory requirements pending the approval of harmonised implementing rules for all member states.

This document is subject to a **permanent evaluation and review process**, with periodic updates in accordance with the development of the standards and the different guidelines published by the European Commission and will be updated once the Digital Omnibus amending the European Regulation on Artificial Intelligence is approved.

Revision date: 10 December 2025

Detailed Index

1. Preamble

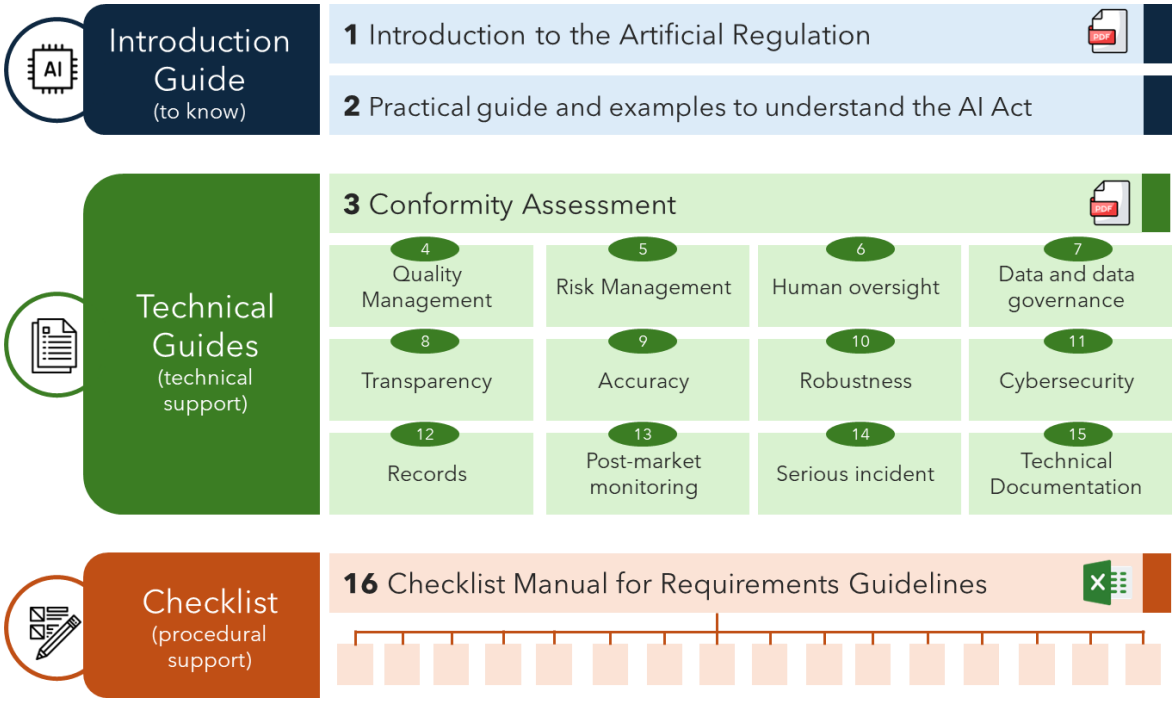
1.1 Objective of the document

The purpose of this introductory guide is to provide a **general understanding of the European Regulation on Artificial Intelligence (AI Act),** providing the reader who is new to the subject with a clear vision of its regulatory scope, its scope of application and the main obligations that derive from it. It aims to serve **as a starting point to familiarise yourself with the essential elements of the Regulation**, addressing in a brief and structured way the key concepts that underpin its content. In this sense, the regulatory context in which the AI Act is inscribed, its purpose within the European legal framework and the implications it has for the different actors involved in the development, implementation and use of artificial intelligence (AI) systems will be presented.

Throughout the following sections, the **scope of application of the Regulation**, **supervisory governance**, the **roles and responsibilities** in the value chain of AI system development defined by the Regulation are identified, as well as the correspondence between the **types of AI systems and the levels of demand that are applicable to them**. Similarly, a **summary of the most relevant obligations is offered according to the level of risk of the system**, accompanied by a brief description.

For those individuals or entities that wish to delve into specific aspects, such as the obligations required of high-risk AI systems, **specialized technical guides** are made available on each requirement, complemented by a **Practical Guide and examples to understand the AI Act** which articulates their joint relationship, in order to promote a coherent and complete understanding of the regulatory framework. The guides, which correspond to articles of the AI Act, are developed in such a way that a relationship can be established between them, as illustrated in the following image:

ILLUSTRATION 1: LIST OF GUIDES OF THE RIVER



This guide takes as a reference Regulation 2024/1689 of the European Parliament and of the Council, of 13 June 2024 (European Regulation on Artificial Intelligence).

2. Introduction

2.1 Introduction to the European Regulation on Artificial Intelligence

The rapid **expansion of artificial intelligence (AI)** has transformed the way organizations approach data management, process automation, and decision-making. Its ability to analyze large volumes of information, identify patterns, and generate accurate predictions makes it an **essential tool for efficiency and innovation across multiple industries.** However, along with its advantages, there are also important ethical, social and legal challenges that require special attention.

The peculiarities that resemble AI systems to humans – especially in terms of autonomous decision-making – have raised **concerns about both the potential societal impacts and the risks inherent in their use**. These include the excessive delegation of critical decisions (for example, in the medical or legal field) or the appearance of biases that can lead to discrimination based on sex, race or age. For this reason, it is **necessary to establish safety and quality requirements for AI systems**, **depending on their degree of risk,** in order to promote the safe use of this technology and minimise possible damage.

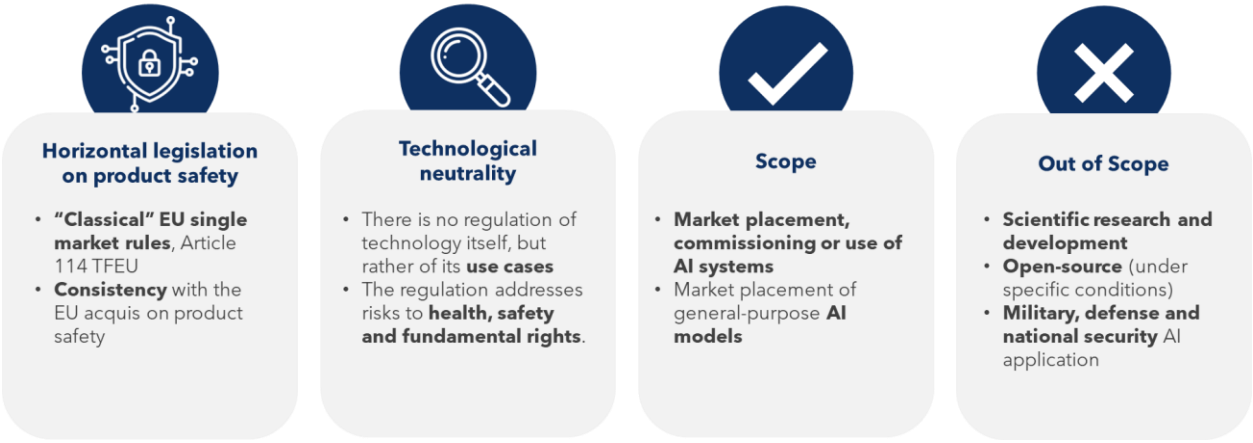
Along these lines, **international organizations such as UNESCO, the OECD and the European Union agree that the human being must always remain at the centre of technological development**, maintaining AI as a tool of support and complement. The principles for defining a secure framework for the use of artificial intelligence are based on this principle:

- **Avoid bias and non-discrimination.** Prevent algorithms from having discrimination problems and look for ways to make the results obtained explainable.
- **Cybersecurity, robustness and accuracy.** Ensure that AI systems are robust against cyberattacks, tampering, or unauthorized alterations, and that they maintain stable, predictable, and accurate behaviour even under adverse conditions.
- **Quality management system and risk management system.** Implement an integrated framework that ensures the documentation, traceability, testing, and ongoing maintenance of systems and that allows for the identification, assessment, and mitigation of risks to health, safety, and fundamental rights, and applies preventive and corrective controls throughout the system's lifecycle.

With the aim of guaranteeing the safety and reliability of systems, while promoting an ethical and responsible use of AI, the European Union has developed the **European Regulation on Artificial Intelligence**, whose general purpose is to ensure the proper functioning of the internal market by establishing requirements that must be implemented during the development and use of AI systems. In other words, this Regulation seeks to create an **ecosystem of trust** based on a legal framework that promotes responsible innovation and the protection of fundamental rights.

The European Regulation on Artificial Intelligence defines the following **regulatory content or scope**:

Illustration 2: Contextualization of AI Act



On the other hand, there are the objectives of the AI Act, which express the **goals or purposes** that the European Union seeks to achieve through this regulation. Among them are:

- **Ensure that AI systems** placed on the market or put into operation in the European Union **are safe** and respect existing legislation and EU values.
- Provide legal certainty to **encourage investment and innovation**.
- Improve governance and effective enforcement of **fundamental rights and safety regulations in the use of AI.**
- **Define a single market for AI**, enabling a reliable and secure use of artificial intelligence, avoiding regulatory fragmentation.

In this way, ethics and regulation are presented as complementary pillars: the first guides the responsible development of technology, and the second establishes the necessary regulatory framework to guarantee its safe and reliable use for the benefit of society as a whole.

Article 2 of the AI Act precisely defines its **limits of application**, establishing which artificial intelligence systems are outside its scope. These exclusions seek to balance the regulation of AI systems with the need to protect sensitive activities and encourage technological innovation. The main areas excluded include:

1. **Research and development (R+D).** The Regulation does not apply to AI systems or models that are developed specifically for the sole purposes of scientific research and development. Nor shall it apply to any research, testing or development activities relating to AI systems or AI models prior to their placing on the market or putting into service. Tests under real conditions will not be covered by this exclusion.

2. **Military, defense or national security.** AI systems used exclusively for military, defence or national security purposes fall outside the scope of the AI Act, regardless of the entity using them or where they are placed on the market or put into service. This exclusion also extends to AI systems that are not placed on the market in the Union, but whose product is used within the Union solely for those purposes.

3. **Open *source- software*.** AI systems released under free or open-source licenses are not subject to the RIA, unless they are marketed or put into service as high-risk AI systems or as systems with transparency obligations. They may not be used for the purposes prohibited by the Regulation.

4. **Use by natural persons in a non-professional field.** The Regulation does not apply to the use of AI by natural persons using AI systems in the exercise of a purely personal activity of a non-professional nature.

2.2 Market Surveillance Governance

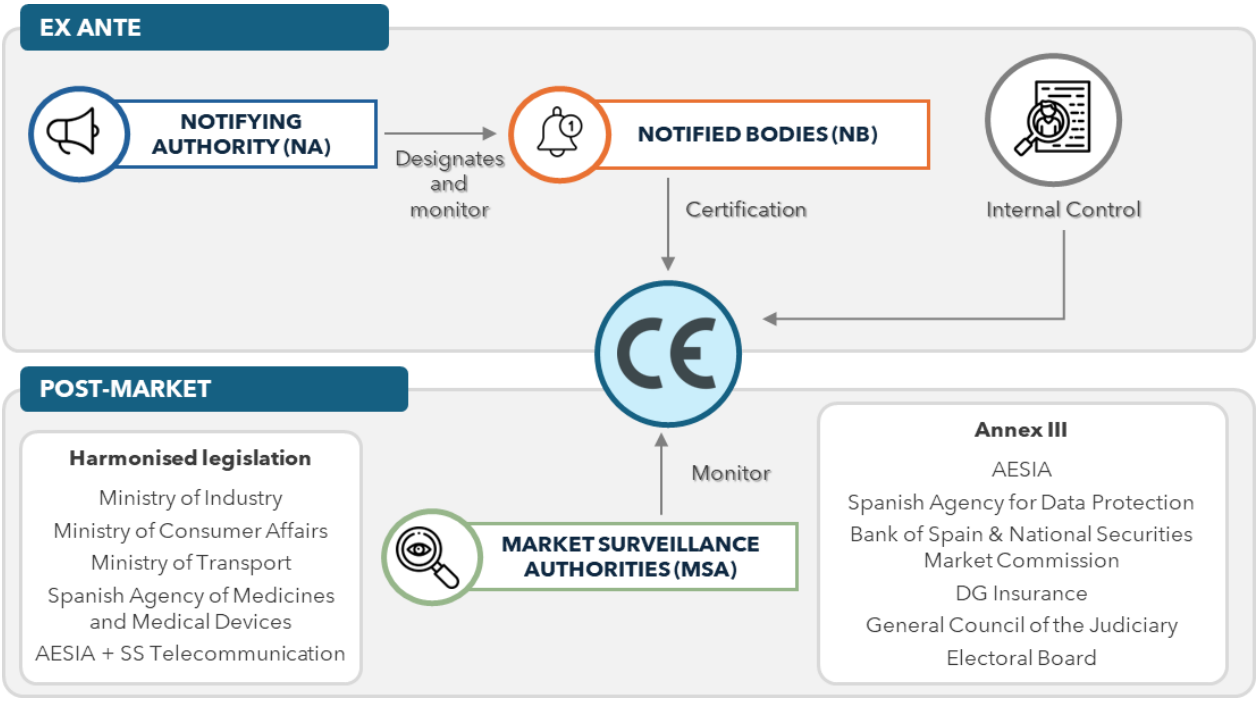
Governance under the European Regulation on Artificial Intelligence is structured on a multi-level model that combines European and national surveillance, with the aim of ensuring the correct application, control and consistency of the AI Act in all Member States. Specifically, each member state must designate a number of National Competent Authorities: the Market Surveillance Authorities (MSAs) and the Notifying Authorities (NAs).

Market Surveillance Authorities (MSAs) play an operational role in controlling, inspecting and monitoring compliance. They are responsible for verifying that the AI systems placed on the market or in service meet the established requirements and may impose corrective or sanctioning measures in the event of non-compliance.

The Notifying Authorities (NAs) shall be responsible for establishing and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies, as well as their surveillance. These authorities may only notify those bodies that have complied with the specific requirements established by the AI Act itself.

In addition, although they are not National Competent Authorities, the so-called **Notified Bodies (NB)** also play an important role. These are those conformity assessment bodies independent of high-risk AI systems that have been duly notified by the NA. Its role is to ensure a technical and objective verification of compliance with the applicable requirements prior to the placing on the market or commissioning of the system in accordance with Annex VII in cases where the involvement of a third party is necessary.

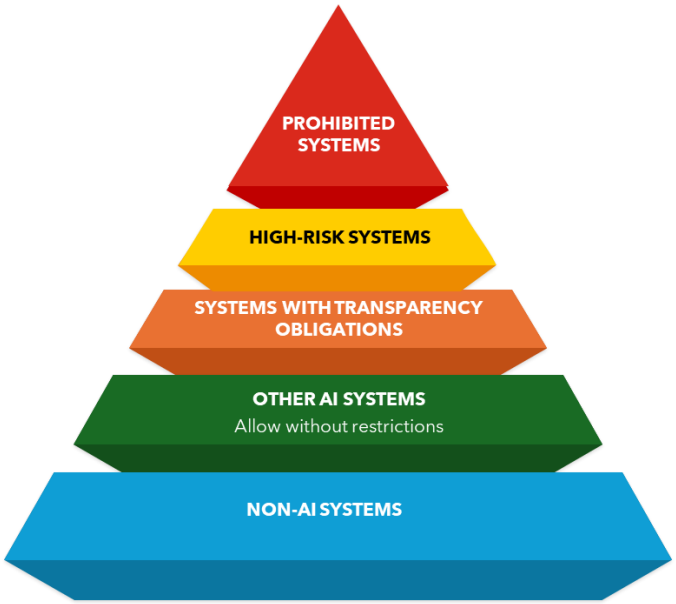
ILLUSTRATION 3: AI ACT GOVERNANCE



2.3 Risk levels of the European Regulation on Artificial Intelligence

The AI Act does not regulate the technology itself - which will allow it to remain in force in the face of the expansion of the technical frontier - but the use made of it. It is **a risk-based regulation of each AI system,** so that the greater the risk, the greater the control. Thus, it establishes the following classification:

ILLUSTRATION 4: CLASSIFICATION OF AI SYSTEMS ACCORDING TO RISK



A) Prohibited systems: uses of AI that are at this level of the hierarchy are prohibited due to the high risk they entail: AI systems that pose a threat to safety, life or fundamental rights. At this level are, for example, systems with any of the following functions:

- Subliminal manipulation of a person's behaviour in a way that may cause physical or psychological harm to him or others.
- Exploiting the vulnerabilities of social groups to manipulate their behaviour in a way that may cause harm to them or others.
- Evaluation or classification of people or groups by their social behaviour that may disproportionately harm them in the area of the behaviour observed, or harm them in areas other than where it was observed.
- Real-time biometric identification in public access spaces for police authorities, except in assessed cases and with authorization.

The European Commission has prepared guidelines to clarify the interpretation of certain specific cases (*Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 20241689 (AI Act)*). [1]

B) High-Risk Systems: the second level is reserved for high-risk systems, but whose use is permitted, to which the AI Act dedicates most of the requirements and obligations that must be met by the different roles involved in the value chain of the implementation of an AI system (operators). They are divided into two types of systems:

B1) High-risk safety products or components covered by harmonisation legislation:

- AI systems that are a safety component of one of the products covered by the Union harmonisation legislation set out in Annex I to the AI Act or,
- That the AI system itself as a product must be subject to a third-party conformity assessment for its introduction on the market or putting into service in accordance with said harmonisation legislation.

In both cases, the **conformity assessment of the AI system** shall be carried out **as part of the conformity assessment of the product** in accordance with the applicable harmonisation legislation.

The harmonisation legislation for each of the products or product safety components is mentioned in **Annex I Section A** of the European Regulation on Artificial Intelligence. **These products are**: machines, toys, lifts, protective equipment and systems for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cable transport installations, appliances that burn gaseous fuels, medical devices, in vitro diagnostic medical devices, automotive and aviation.

In the context of conformity assessment, where the legislative acts in Section A of Annex 1 allow the manufacturer to dispense with the assessment of a third party, provided that the manufacturer has applied all the harmonised standards covering all the relevant requirements, **that manufacturer may only use this option if he has also applied the**

[1] Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 20241689 (AI Act)

harmonised standards, or, where appropriate, the common specifications referred to in the AI Act.

B2) High-risk purposes:

AI systems that are used for purposes that are considered to present a high risk to the health, safety and/or fundamental rights of individuals, taking into account both the seriousness of the potential harm and the likelihood of it occurring.

These purposes are mentioned in **Annex III** of the European Regulation on Artificial Intelligence. Specifically, **these purposes are:** biometrics, critical infrastructures, vocational education and training, employment, worker management and access to self-employment, access to essential private services and essential public services and benefits, ensuring compliance with the law, migration, asylum and border control management and administration of justice and democratic processes.

In the context of conformity assessment, **the high-risk systems listed in Annex III, point 1**, the supplier has applied the harmonised standards, or common specifications **may opt for a conformity assessment procedure with the involvement of a notified body or based on internal control** (self-assessment), while **the systems of points 2 to 8 will comply with the latter**.

C) Systems with transparency obligations: The regulation establishes the obligation of transparency towards users for this type of product. Among other things, they are obliged to make it clear that their departure is the product of an artificial intelligence system, not a human. At this level are *chatbots* and deep fake *creation systems*, among others.

In the case of these systems, the **obligation is established to inform the users** of these systems that they are carrying out an interaction with an AI system, and not a human being, in addition to the **labelling of all synthetic content (video, audio, text, etc.),** generated through AI.

D) Other AI systems: for the rest of the AI systems, only basic obligations are contemplated, such as training users of the systems in AI (literacy). Among them is the application of AI to video games or spam filters for email.

E) Non-AI systems: certain more classical algorithms, such as those based on rules or heuristics, are not considered AI systems under the Regulation, and therefore do not apply to them.

The AI Act also regulates **general-purpose AI models (GPAI),** AI models that are typically trained with a large volume of data and that are capable of competently performing a wide variety of different tasks such as answering questions, translating, generating all kinds of content, etc. These models **can be adapted to a wide variety of tasks through configuration or subsequent training**. Depending on its integration into a purpose-driven AI system, the system may be considered high-risk or even prohibited use.

Depending on their size and the risks arising from their use, we speak of general-purpose AI models and general-purpose AI models of systemic risk. Differentiated obligations are established for these models ranging from:

- Transparency obligations.

- Preparation of technical documentation.
- Guidelines on Copyright Compliance.
- Model evaluation, risk mitigation, recording and communication of serious incidents.

AI Act is more flexible in terms of regulatory obligations for general-purpose AI models that are open source or free license.

To facilitate compliance with the requirements imposed on providers of general-purpose models, the Commission has published a general-purpose AI code of practice[2] composed of three chapters: transparency, intellectual property and security. This code is accompanied by guidelines[3] for suppliers of this type of model. Through these tools, the AI Office seeks to provide a framework of certainty that guarantees regulatory compliance with the GPAI.

2.4 Operators under the European Regulation on Artificial Intelligence

The **European Regulation on Artificial Intelligence** mentions all potential **roles involved in the value chain of AI systems (operators).** The goal is to establish the responsibilities that each of these roles must assume during the life cycle of AI systems.

2.4.1 Definitions of operators under the AI Act

Provider
A natural or legal person, public authority, agency or other body that **develops or causes to be developed an** AI system or a general-purpose AI model **and places it on the market or puts it into service under its own name or trademark**, whether for consideration or free of charge.
Deployer
Any natural or legal person, public authority, body or any other entity that **uses an AI system under its authority**, except when such use is part of a personal activity of a non-professional nature.
Authorised 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 comply with the obligations** and carry out the procedures set out in this Regulation on behalf of that provider.

[2] https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
[3] https://ec.europa.eu/newsroom/dae/redirection/document/118340

Importer
Any natural or legal person physically present or established in the Union who **places on the market an AI system bearing the name or trademark of an AI system from a natural or legal person established outside the Union**. They place on the market for the first time the AI system to market in the name or trade mark of a natural or legal person established outside the Union, whether the supply is paid or free of charge.
Distributor
Any natural or legal person in the supply chain, other than the supplier or importer, who places an AI system on the Union market. They place the systems on the market, i.e. **they supply an AI system for distribution or use on the Union market** in the course of a commercial activity, whether the supply takes place on a paid or free basis.

2.4.2 When does a deployant or other persons become required to comply with vendor obligations?

The Regulation contemplates various circumstances in which different subjects other than the supplier assume the obligations that a priori are assigned to the latter.

Specifically, any distributor, importer, deployant or third party **will be considered a provider** of a new high-risk AI system for the purposes of the Regulation **if any of the following circumstances occur:**

- **They put their name or brand** on a high-risk AI system that has **already** been **placed** on the market or put into service, without prejudice to contractual arrangements that stipulate that obligations be assigned in another way.

- **They make a substantial modification of a high-risk AI system that has already been placed on the market or put into service.**

- **They change the intended purpose of a** non-high-risk AI system that is already placed on the market or put into service, **so that** the modified system becomes a high-risk AI system.

Attention should be drawn to the importance of these situations of modification of the intended purposes or alteration of the intended purpose.

This will obviously have clear implications for the responsibilities of both subjects. Where these circumstances apply, the provider that initially placed on the market or put into service the

high-risk AI system shall cease to be considered a provider for the purposes of the Regulation, if those changes have been made by another operator.

2.4.3 Individuals of public sector operators

As a general rule, **the Regulation applies equally to private organisations, public administrations and public sector entities**. However, the additional obligation for a high-risk system is established, which consists of the development of an **impact assessment relating to fundamental rights**.

With the aim of effectively guaranteeing the protection of fundamental rights by determining the specific risks to the rights of the individuals and groups that are affected.

EIDF or FRIAs (Impact Assessment relating to fundamental rights)
Mandatory **prior to deployment** of a high-risk system* Carried out by **deployment managers.**
Content • Description of the system's use processes. • Time period and frequency of use. • Category of affected individuals and groups. • Specific risks of harm. • Description of human oversight measures. • Measures in case the risk materializes (Grievance mechanisms).
System used in **similar cases**, responsible for deployment **based on previously or existing EIDFs.** Some of the **content already included in the DPIA** (Data Protection Impact Assessment), **EIDF will complement it.**
Notification to AESIA (Pending publication of the questionnaire model by the AI Office)

*Exception: Critical Infrastructures

2.4.4 Small and medium-sized enterprises (SMEs), including start-ups[4]

The AI Act pays particular attention to small and medium-sized enterprises, including start-ups that are providers and responsible for the deployment of AI systems.

Thus, various obligations are foreseen to be adopted by both the European Commission and the Member States in favour of these organisations when they assume the role of deployment

[4] Most of the particularities applied to SMEs in the regulation are extended to small mid-cap enterprises (SMCs) in the text of the Digital omnibus submitted to the European Parliament. These are defined as those which, not being SMEs, have fewer than 750 employees and whose annual turnover does not exceed EUR 150 million or whose annual balance sheet does not exceed EUR 129 million.

managers or suppliers. Facilitating compliance with the Regulation by adapting the obligations according to its capacity and size, guaranteeing a correct final security of the AI system.

One of the particularities of SMEs derives from the sanctioning regime. Generally, when an organisation is penalised in accordance with the Regulation, the fine imposed should be the greater of the amounts corresponding to the total amount allocated to that infringement or the specific percentage allocated to that infringement in relation to the turnover of that organisation. However, in the case of SMEs, the fine imposed may be the lower of the amounts of the amounts previously indicated.

The image below identifies some of the particularities foreseen for small and medium-sized enterprises in the AI Act.

ILLUSTRATION 5: PARTICULARITIES SMES, EMERGING COMPANIES AND START-UPS

Particularities of SMEs, start-ups and start-ups
• Penalties in the lower amount between the amount or percentage (see previous text). • Priority access to sandboxes. • Specific channels for advice and consultations. • Standardised forms for compliance with the regulation. • Reduction of technical documentary burden and fees during the conformity assessment process. • Quality Management Systems adapted proportionally to the size of the company.

2.5 AI regulatory sandboxes

Article 57 of the AI Act develops the regulation for the establishment of **sandboxes for artificial intelligence, with the aim of supporting innovation in AI.** These are controlled test environments, supervised by competent authorities that foster innovation and facilitate the development, training, testing and validation of innovative AI systems for a limited period before they are placed on the market or put into service.

At the request of the provider, the sandbox competent authority will provide an exit report detailing the activities carried out and the results. This documentation may be used by suppliers to demonstrate their compliance with the Regulation through the conformity assessment process or relevant market monitoring activities. **MSAs and NBs shall take positive account of reports and tests, with a view to speeding up the procedures** to a reasonable extent, without this implying an exemption from obligations or replacing formal conformity assessment procedures.

3. Main Obligations

This section details some of the most important obligations of the AI Act for different operators.

3.1 AI literacy obligations

A series of general obligations are contemplated applicable to all entities that act as providers or responsible for the deployment of AI systems in terms of literacy in the organization.

According to Article 4, any entity that places on the market or uses AI systems must promote AI literacy. To do this, it must be ensured that **the personnel in charge of operating the systems have sufficient knowledge of Artificial Intelligence**.[5]

3.2 Transparency obligations

Article 50 lays down transparency obligations, requiring **providers and those responsible for deployment to provide clear and understandable information** when people interact with an AI system, when synthetic content (e.g. text, images or video) is generated, or when emotional or biometric recognition techniques are used. In such cases, it will be necessary to indicate the use of an AI system:

- When a system interacts directly with natural persons, it must be reported that it is interacting with an AI system.
- Where a general-purpose AI system generates synthetic content, it shall be ensured that the content is marked in a machine-readable format and that it is detectable that it has been artificially generated or manipulated.
- Those responsible for the deployment of an AI system that generates *deepfakes*, will make public that the content has been generated or manipulated artificially.
- Those responsible for deploying an AI system that generates or manipulates text that is published for the purpose of informing the public about matters of public interest shall disclose that the text has been artificially generated or manipulated.

3.3 Obligations of high-risk systems

The obligations that must be met by **providers** of high-risk systems under the AI Act are concisely described below:

Risk management system (Article 9)
A risk management system aims to identify and analyze risks and implement measures to mitigate their impact. In the context of the European Regulation on Artificial Intelligence, the risk management system shall pay particular attention to the **identification, analysis, assessment and mitigation** of **risks affecting the health, safety and fundamental rights of individuals,** both in their intended use and in reasonably foreseeable uses. The Regulation also include monitoring mechanisms, testing, and systematic updates, with an emphasis on technical mitigation, proper design, and training of those responsible for deployment. The

[5] According to the text of the Digital omnibus submitted to the European Parliament, the obligation of literacy is replaced by encouraging all users of the system to have knowledge and adequate training in AI.

risk management process must be addressed at all stages of the AI system's lifecycle, from design and development to commercialization and post-commercialization.

For more information, see the Risk Management Guide.

Data and data governance (Article 10)

In the context of AI, **data governance is the set of elements** (policies, procedures, processes, standards, etc.) **which are implemented to ensure that the data used in the training, validation and testing of AI systems is adequate**, relevant, sufficiently representative and meets the established quality and completeness requirements.
The European Regulation on Artificial Intelligence establishes a series of requirements that must be met mainly by the provider of a high-risk AI system, including **organizational and technical measures** that will serve providers and those responsible for the deployment. These measures apply in **each of the phases of the proposed data management model in order to implement adequate data governance**: information requirements, data collection, preparation, data availability, data elimination, and monitoring and continuous improvement.

For more information, see the Data and Data Governance Guide.

Technical documentation (Article 11)

In order to **enable the traceability of high-risk AI systems**, **to verify** whether they comply with the **requirements** of the Regulation, as well as **to monitor their operation and carry out post-market monitoring**, it is essential to have understandable **technical documentation** on how they have been developed and on their operation throughout their lifetime. This technical documentation plays a very important role within the conformity assessment framework.
When complying with this obligation, it is important to define **how to reflect and structure this documentation, and how it should be preserved**.
This obligation is complemented by the obligation to register any high-risk system referred to in Annex III in an EU database (Article 49), except for those relating to critical infrastructures, which will be registered in a national register due to their criticality for national security.

For more information, see the Guide to technical documentation and documentation conservation.

Record-keeping (Article 12)

A **log is a file that stores information about the behaviour and performance of the system** during training or production use. Therefore, a **log management system is a set of processes that are defined to collect, store, analyze, and manage the logs** generated by an AI system.
The logs allow developers and operators of the system to understand how it behaves in different situations and how it can be optimized to improve its accuracy and efficiency. It can also help detect errors or biases in the system.
It is necessary to address the development of an adequate records management system, which will not only make it possible to comply with the requirements of the Regulation, but will also **facilitate** other tasks such as **transparency and accountability, and other evidence-based research and development activities.**

For more information, see the Guide to logs and auto-generated log files.

Transparency (Article 13)

Transparency is the quality of an **AI system being able to be interpretable and understandable by all the people** who create it and interact with it throughout its life cycle. The European Regulation on Artificial Intelligence establishes the obligation to ensure the design and development of systems that allow those responsible for the deployment to **understand and use the system appropriately; to provide instructions for use** that include concise, complete, correct and clear information that is relevant, accessible and understandable to those responsible for the deployment; as well as a **set of specific information to be taken into account in the design and development of the system**.

For more information, see the Transparency and Disclosure of Information to Users Guide.

Human Oversight (Article 14)

People need to be able to keep an eye on the operation of high-risk AI systems. To this end, systems must provide the **necessary tools and interfaces to exercise this supervision** and interact with them in a secure manner. In other words, human oversight helps ensure that an AI system does not undermine human autonomy or cause other adverse effects.
The measures are therefore specifically aimed at the specific design and development of high-risk AI systems, so that they allow effective monitoring to be carried out on them; the establishment of mechanisms for the prevention and minimization of risks (on health, safety, and fundamental rights); the location of the responsibility of suppliers and those responsible for the deployment; informed and aware monitoring of the system; and ensuring human oversight in those systems that make use of biometric identification.

For more information, see the Human oversight Guide.

Accuracy (Article 15)

A keyway to be able **to mitigate the risks in the use of AI as much as possible is to improve the accuracy of this AI system**. Through the accuracy of the system, we obtain a quantitative measure of the relationship between the **intended purpose of the system and its performance** from design to operation after the implementation of the AI system.
This is achieved through a series of **measures aimed at ensuring that AI systems do not degrade their performance and accuracy specifications once they are put into operation**. To do this, they must respect minimum levels of accuracy and/or specific metrics associated with the task, pre-established, thus ensuring that it is consistent throughout the life cycle.

For more information, see the Accuracy Guide.

Robustness (Article 15)

Technical robustness is understood as the resilience of the system in relation to harmful, or otherwise undesirable, **behaviour that may result from limitations in the systems or in the environment in which they operate** (e.g. errors, failures, inconsistencies or unexpected situations). For this reason, it establishes that the AI system must consider, in its **design, development and validation, the technical and organizational solutions to prevent such situations**, foreseeing the possibility that when such technical robustness does not operate within safe parameters, the system may even interrupt its operation.
It is **the responsibility** of the high-risk AI system provider to take appropriate measures (both organizational and technical) to ensure that the system's robustness requirements are met. Likewise, within its scope of application, the **person responsible for the deployment of the system also has responsibilities** that will materialize in specific measures (again organizational and technical).

For more information, see the Robustness Guide.

Cybersecurity (Article 15)

Cybersecurity in high-risk Artificial Intelligence systems is a key aspect of its design, as these are systems that are exposed to specific threats that require rigorous protection measures adapted to their context.
The built-in cybersecurity measures required of a high-risk AI system aim to **mitigate risks that threaten the rights and freedoms of individuals and society at large** and are integrated into broader cybersecurity management frameworks. These can be seriously threatened by the existence of backdoors in the models, the possibility of exfiltration attacks or vulnerability to adversarial attacks.

For more information, see the Cybersecurity Guide.

Quality management system (Article 17)

Article 9 of the AI Act '*Quality Management System*' lays down quality requirements to be met by suppliers of high-risk AI systems in order to **implement a documented quality management system** to ensure regulatory compliance. This system should include **compliance strategies, risk management, design and development control, testing, post-market monitoring, incident reporting, and communication with authorities and stakeholders**. Its scope should be proportional to the size of the provider and can be integrated with existing systems if it complies with EU industry regulation.

For more information, please refer to the Quality Management Guide.

Conformity assessment (Article 43)

The European Regulation on Artificial Intelligence establishes that according to Article 43, high-risk artificial intelligence systems must undergo a conformity assessment procedure prior to their market placing or commissioning. This procedure distinguishes between **internal**

control and third-party evaluation, depending on the nature of the system and the application of harmonised standards.

The high-risk AI systems that are subject to the **internal control-based assessment procedure defined in Annex VI** are those listed in points 2 to 8 of Annex III. This procedure allows the supplier to carry out an internal control, verifying compliance with the essential requirements set out in the Regulation and the adequacy of its quality management system in accordance with Article 17.

The systems referred to in point 1 of Annex III, particularly those relating to remote biometric identification, may be subject to the same internal control-based procedure referred to. However, they shall be subject to the conformity assessment procedure with the intervention of a notified body where harmonised standards or common specifications have not been applied, as provided for in **Annex VII.**

In addition, in cases where the AI system is part of a product covered by Union sectoral harmonisation legislation (referred to in Annex I, Section A), the conformity assessment shall be integrated into the procedure established for that product, applying the provisions of Article 43(3) together with the technical criteria defined in Annexes VI and VII.

For more information on conformity assessment processes, see Annex I to this Guide and the Conformity Assessment Guide.

Post-market monitoring (Article 72)

The European Regulation on Artificial Intelligence introduces the need for a monitoring system to be established after the implementation of high-risk AI systems, as part of a post-market monitoring plan.
A post-market monitoring plan is a **set of activities conducted by suppliers/users**, to collect and evaluate the experience obtained from high-risk artificial intelligence systems that have been **put on the market** and thus identify the need to take any action. This is an important tool to ensure that AI systems remain secure and function properly. The **evaluation carried out with this post-market monitoring can also contribute to a continuous improvement of the system**.

For more information, see the Post-Market monitoring Guide.

Reporting of serious incidents (Article 73)

The Regulation defines as an obligation of HRAI providers the need **to report any serious incident or defect of an AI system to market surveillance authorities.** The notification of serious incidents will entail the establishment of coordination with the European authorities by the competent national authorities, with the aim of controlling and monitoring the most serious incidents.

For more information, see the Critical Incident Reporting Guide.

3.4 Obligation activation dates

System Type		Date of market introduction or commissioning		Compliance Obligations AI Act
Prohibited		N/A		February 2025
High risk	**Annex I**	Before	2 August 2026	N/A, except if significant changes (August 2027) Twelve months from publication of communication (maximum August 2028)*
		After		August 2027 Twelve months from publication of communication (maximum August 2028)*
	Annex III	Before		N/A, except if significant changes (August 2026) six months from publication of communication (maximum December 2027)*
		After		August 2026 December 2027*
	Used by Public Authorities	Before		August 2030
Supplier Transparency Obligations Art 50(2)		Before	2 August 2026	August 2026 February 2027*
		After		August 2026
Transparency obligations		Before		August 2026
		After		
GPAI		Before	2 August 2025	August 2027
		After		August 2026
		GPAI Modification**		

* Current version of the Digital Omnibus on AI
** Modification > 1/3 training on Base Model published before August 2025

4. ANNEX I. Conformity assessment of high-risk AI systems and Market Surveillance Authorities

This table sets out the different types of conformity assessment depending on the high-risk AI system and the relevant Market Surveillance Authority (MSA). The MSAs indicated take as a reference the designation established by the Draft Law for the Good Use and Governance of Artificial Intelligence, and therefore, their final ratification will depend on the approval of this standard.

	AI Product/System	Market Surveillance Authority	Type of assessment
ANNEX I	Machinery	SG Industrial Quality and Safety. Ministry of Industry. (According to the Draft Law)	Procedure according to product legislation
	Appliances burning gaseous fuel		
	Pressure equipment		
	Cableway systems		
	Personal protection		
	Lifts		
	Protection for use in potentially explosive atmospheres		
	Radio equipment	AESIA in collaboration with the Secretary of State for Telecommunications and Digital Infrastructures. Ministry of Digital Transformation.	
	Toys	DG Consumer Affairs. Ministry of Consumer Affairs. (According to the Draft Law)	
	Pleasure boats	DG Merchant Marine. Ministry of Transport. (According to the Draft Law	
	In vitro diagnostic medical devices	Spanish Medicines Agency. (According to the Draft Law)	
ANNEX III	Critical infrastructures, Education and training, Employment and worker management, Access to public services, Prioritisation of emergency services.	AESIA (According to the Draft Law)	Self-evaluation
	Limited biometric identification		Self-assessment or notified body. Depending on whether or not they apply harmonised standards or

			common specifications.
	Credit Scoring	ECB and CNMV (According to the Draft Law	Self-evaluation
	Insurance premiums	DG Insurance and Pension Funds (According to the Draft Law	Self-evaluation
	Biometric identification for law enforcement and border management	AEPD (According to the Draft Law	Self-assessment or notified body. Depending on whether or not they apply harmonised standards or common specifications.
	Law Enforcement and Border Management		Self-evaluation
	Biometric identification for the Administration of Justice	CGPJ (Still to be defined)	Self-assessment or notified body. Depending on whether or not they apply harmonised standards or common specifications.
	Administration of Justice	CGPJ (According to the Draft Law)	Self-evaluation
	Biometric identification for democratic/electoral processes	Electoral Board (Still to be defined)	Self-assessment or notified body. Depending on whether or not they apply harmonised standards or common specifications.
	Electoral/Democratic/Electoral Purposes	Electoral Board (According to the Draft Law)	Self-evaluation

Financiado por
la Unión Europea
NextGenerationEU