2

Guide 2. Practical guide and examples to understand the AI Act

European
Artificial Intelligence Act

Companies that are beginning to know the

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 Artificial Intelligence Act is approved.

Revision date: 10 December 2025

Detailed Index

1. Preamble

1.1 Purpose of the document

The aim of this guide is to facilitate the understanding of the AI Act from a practical approach. To this end, an introductory context of the technical guides is provided, as well as hypothetical examples of high-risk systems and AI that are used throughout the guides with a didactic objective that helps to improve their understanding.

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).

1.2 How to read this guide?

This guide should be read in a complementary way to the Introduction to the IA Act, in order to introduce the technical guides and help to clarify some of the most common doubts that have arisen during the participation in the Spanish Sandbox IA pilot.

The **first section** contains the preamble, where the general purpose of the guide is presented.

The **second section** provides summaries of the examples of the use cases that are used as examples throughout the technical guides to illustrate their practical application.

The **third section** contains a glossary of some of the most relevant general terms and concepts (taken from Article 3 of the RIA) to facilitate the practical understanding of the Regulation, accompanied by examples linked to the aforementioned use cases.

In the **fourth section** , it provides a context on the development of the Spanish Sandbox IA pilot, in which the technical guides emerge, as well as a relationship between the guides and the obligations of high-risk systems, in order to facilitate their consultation.

1.3 Who is it for?

To companies and individuals who wish to improve their understanding of the AI Act and plan to use or consult the technical guides.

2. Examples of AI Systems

This section presents several examples of AI systems, in the form of patterns, that have been selected for their representativeness. Throughout all the guides and documentation provided during the sandbox, these use cases will be used as a cross-cutting example, to facilitate the explanation and understanding of the different sections. All use cases presented in this section are high-risk.

2.1 AI system for biometric identification at work

Title	Attendance at work
Description	Artificial intelligence system for biometric recognition to record time and attendance at work. It has cameras (or biometric sensors) that record entry, and cameras (or biometric sensors) that record exit, **without active employee participation**. The system associated with each camera records entry/exit times. The intended use is to control the time worked and not the identification or verification, so in this use case, identification is not the only purpose of the system, but the control of the time worked.
Potential Deployants	Any company, to control and monitor the attendance at work of its employees.
RIA Annex	Annex III
Aloof	1 - Biometric systems.
Subsection	a - Biometric systems.

2.2 AI System in Personnel Management – Promotion

Title	Personnel Management - Promotion
Description	This artificial intelligence system evaluates the possible promotion of employees. The system includes a series of parameters to evaluate an organization's employees and determine whether or not they should be promoted to a new position. The promotion proposal provided by the AI system influences as one of the determining factors, and not merely ancillary, in the establishment of the remuneration of the new position.

Potential Deployants	Companies for the management of promotions of their employees, if the service or personnel management is outsourced, may have those responsible for the deployment nested.
RIA Annex	Annex III
Aloof	4 - Employment, worker management and self-employment.
Subsection	b - AI intended to be used to make decisions relating to the promotion and termination of contractual employment relationships, the assignment of tasks and the monitoring and evaluation of the performance and conduct of individuals in the framework of such relationships.

2.3 AI system for predicting the risk of social exclusion and assessing access to aid/subsidies

Title	Prediction of risk of social exclusion and assessment of access to aid/subsidies.
Description	This artificial intelligence system will collect specific data on the family unit, as well as general data on the aid requested. The artificial intelligence system establishes access to aid concession based on the set specific parameters, as well as the general parameters that predict the risk of social exclusion in the short term. In addition to access, the system establishes a range of the amount allocated. Access and the amount allocated is directly determined by the system.
Potential deployment managers	Public administrations to establish access and establish the amount of aid.
RIA Annex	Annex III
Aloof	5 - Access to and enjoyment of essential private services and essential public services and benefits.
Subsection	a - AI systems intended to be used by or on behalf of public authorities to assess the eligibility of natural persons to access public assistance benefits and services, as well as to grant, reduce, withdraw or recover such benefits and services.

2.4 AI System for Chronic Disease Management - Smart Insulin Pump

Title	Chronic Disease Management - Smart Insulin Pump
Description	Artificial intelligence system that administers insulin by monitoring the patient's condition. It monitors the patient's condition by recording parameters such as blood sugar level, activity, pulse or volume of oxygen in the blood. These values are used by the model to predict a trend and deliver insulin automatically. The system is also responsible for managing the sending of alarms to the patient and the doctor.
Potential Deployants	The person responsible for the deployment of the system would be the medical institution or hospital that provides the doctor with the system, which he or she will apply to patients.
RIA Annex	Annex I
Aloof	To
Subsection	11 - Medical devices.

2.5 AI system for the detection of false reports

Title	Detection of false reports
Description	Artificial intelligence system used to know the probability that a complaint filed at a police station is false by taking as a reference the complaint filed by the citizen and transcribed into the system by him or the police.
Responsible for potential deployment	Security forces (both national and regional in each case) that manage and process complaints from citizens.
RIA Annex	Annex III
Aloof	6 - Law enforcement matters.
Subsection	c - AI systems intended to be used by law enforcement authorities for the assessment of the reliability of evidence during the investigation or prosecution of criminal offences.

3. Definitions with examples

This section addresses some of the general concepts and terms described in Article 3 of the most relevant Regulation. All of these terms and concepts are used throughout the development of the rest of the sandbox guides and materials.

This content is intended to serve as a first contact with the terms and serve as a reference throughout the execution of the sandbox. Most definitions are accompanied by examples applicable to the examples of AI systems described above, with the aim of providing context to the terms presented.

The definitions indicated take as a reference the version of the Regulation published by the Council of the European Union on 13 June 2024. Only one of these definitions is not contemplated in the Regulation, it is the concept "life cycle of an AI system", which complements the global understanding of the stages of a system.

3.1 Artificial Intelligence System (AI System)

Artificial intelligence system: a machine-based system that is designed to operate with different levels of autonomy and that can show adaptability after deployment, and that, for explicit or implicit objectives, infers from the input information it receives how to generate output results, such as predictions, content, recommendations or decisions, that can influence physical or virtual environments;

The European Commission has published guidelines that aim to clarify this definition of an AI system[1]

Example - Biometric identification at work
A set formed by the cameras that captures the information and the model that performs the analysis of the data and compares it with the stored information to generate the identification and record the information of the entry or exit event and thus monitor the time worked. This example would be a high-risk AI system of those regulated in Annex III, specifically in section 1.

[1] https://ec.europa.eu/newsroom/dae/redirection/document/118640

Example - Chronic Disease Management - Smart Insulin Pump
Formed by the mechanism of collecting data related to the concentration of glucose in the blood which, together with other attributes stored in the patient's database (physiology of the patient, their history and activities, such as meals and physical activity), analyzes and determines the correct dose of insulin to be administered. This example would represent a high-risk AI system of those regulated in Annex I, namely it would fall within the sectoral legislation on medical devices referred to in paragraph 11 of that Annex.

3.2 Placing on the market

Placing on the market: the first placing on the Union market of an AI system or a general-purpose AI model;

Example
In the defined use cases, the placing on the Union market of the AI systems described would correspond to the first time that such a system is put into service and used, developed or imported by a natural or legal person physically present or established in the Union.

3.3 Making available on the market

Making available on the market means the supply of a general-purpose AI system or AI model for distribution or use on the Union market in the course of a commercial activity, subject to payment or free of charge.

In the defined use cases, the placing on the market of the AI systems described would correspond to the moment at which those systems are placed for distribution or use on the market within the Union, either for remuneration or free of charge. In such a way that any of its potential managers for the deployment could acquire it and launch it.

Example – Chronic Disease Management – Smart Insulin Pump
When available and the provider has been contracted by those responsible for the deployment such as hospitals to distribute to their patients.

3.4 Intended purpose

Intended purpose: the use for which an AI system is designed by a supplier, including the specific context and conditions of use, as provided by the supplier in the instructions for use, promotional and sales materials and declarations, and technical documentation.

Example – Biometric identification at work
Its intended purpose would be the identification of employees to record the time of departure and entry, by extracting biometric patterns through the entry/exit cameras and comparing them with previously registered identities. Additionally, it should be explained that this system makes a complete reading of the employee's face, and that, once this data has been identified and collected, the system will carry out a comparison work with the information stored in the database and will analyze whether the traits it has identified correspond to any of those stored in the database. identifying the person responsible for the deployment and recording the corresponding entry or exit event.

3.5 Safety Component

Safety Component: a component of an AI product or system that performs a safety function for that AI product or system, or whose failure or malfunction endangers the health and safety of persons or property;

Example – Chronic Disease Management – Smart Insulin Pump
The AI system collects the data regarding the blood glucose concentration that it analyzes along with other attributes stored in the patient's database and determines the correct dose of insulin to be administered. In this context, the security of these systems is crucial since a failure of any kind can endanger the life of the person responsible for the deployment of the system. An example of a safety component is a sensor that warns of the failure of the insulin pump in case it does not operate properly or is not even operational. The system will be equipped with a large number of safety components, but all of them must clearly notify the person responsible for deploying the device of their malfunction.

3.6 Substantial modification

Substantial modification means a change to an AI system after its introduction into the market or entry into service that was not foreseen or projected in the initial conformity assessment carried out by the provider and as a result of which the AI system's compliance with the requirements set out in Chapter III is affected; section 2, or that results in a modification of the intended purpose for which the AI system concerned has been evaluated;

In any of the use cases presented, in particular, the change of purpose or purpose of the system to another high-risk purpose will be a substantial modification. Similarly, the modification of the system that could affect compliance with the requirements of the Regulation that have previously been assessed for compliance (risk management system, data and data governance, technical documentation, event registration, transparency towards those responsible for deployment, human oversigth, accuracy, robustness and cybersecurity) will be substantial.

Example – Detection of false reports
The initial purpose of the system is to know the probability that a complaint filed at a police station is false. A substantial modification could occur in the event that the system is used in investigations to evaluate the veracity of the statements of the persons under investigation. Or that the introduction of texts of interactions on social networks is practiced to determine patterns of falsehood in these contexts.

3.7 Post-market monitoring system

Post-market monitoring system: all activities carried out by providers of AI systems aimed at collecting and reviewing the experience gained from the use of AI systems that they place on the market or put into service, in order to detect the possible need to immediately apply any type of corrective or preventive measure that may be necessary.

Example – Chronic Disease Management – Smart Insulin Pump
The system provider shall have a procedure for monitoring the product after it has been placed on the market, collecting data and information about the behaviour of the system and opinions of those responsible for the deployment that will enable it to identify, for example, possible errors in the operation of the system and correct it. This post-market monitoring will involve the notification of incidents to the market surveillance authority and substantial modifications to the artificial intelligence system.

3.8 Common Specification

Common specification means a set of technical specifications as defined in point (4) of Article 2 of Regulation (EU) No 1025/2012 which provides means to comply with certain requirements laid down under this Regulation;

In general, and following Regulation (EU) No. 1025/2012, a technical specification is a document that prescribes the technical requirements that a product, process, service or system must meet. The technical specification refers to aspects such as quality, performance, interoperability, environmental protection, health and safety, product dimensions, name, testing, test methods, packaging, marking or labelling, and conformity assessment procedures.

In the context of the Regulation, and with respect to the common specifications, it is indicated:

1. If **harmonised standards** do not exist (or where the Commission considers them insufficient), the Commission may adopt **common specifications** in relation to the **requirements of Section II of Chapter 3**.

2. When developing the **common specifications**, the Commission **shall seek** the **views of** the relevant bodies or groups of experts (established in accordance with applicable Union law at sectoral level).
3. High-risk AI systems conforming to the common specifications shall be presumed **to** be in compliance with the **requirements of Chapter 3, Section II** (to the extent that those common specifications provide for those requirements).
4. Where suppliers do not comply with the **common specifications**, they shall duly justify that they have adopted **technical solutions** at least **equivalent** to them.

Common specifications are developed by the European Commission. For example, there are common specifications in Regulation 2017/745, of 5 April, on medical devices, to implement the requirements that are required of certain medical devices.

3.9 Training Data

Training data: The data used to train an AI system by adjusting its trainable parameters.

Example – Prediction of risk of social exclusion and assessment of access to aid/subsidies
The data with which the system will be trained are the stored data associated with the different parameters, both quantitative (income level, level of education, occupation, geographical areas, etc.) and qualitative (typified reports, textual reports). That is, all the performance data – granted or not – that is selected, to develop the artificial intelligence system, as data used during its training.

3.10 Validation Data

Validation data: the data used to provide an assessment of the trained AI system and adapt its non-trainable parameters and learning process to, among other things, avoid underfitting or overfitting;

Example – Prediction of risk of social exclusion and assessment of access to aid/subsidies
Validation data are data that allow us to evaluate the system we have trained, these data also belong to the stored data associated with the different parameters, both quantitative (income level, level of training, occupation, geographical areas, etc.) and qualitative (typified reports, textual reports), it can be a subset of the data used in the training or another subset of data from that history that was not used in the training phase.

3.11 Testing Data

Testing data: the data used to provide an independent assessment of the AI system, in order to confirm the intended operation of the AI system before it is placed on the market or put into service.

Example – Prediction of risk of social exclusion and assessment of access to aid/subsidies
Test data is data that allows us to independently evaluate the trained and validated system. This dataset must be different from the one used for training and validation but sharing exactly the same nature: stored data associated with the different parameters, both quantitative (income level, level of education, occupation, geographical areas, etc.) and qualitative (typified reports, textual reports).

3.12 Input Data

Input data: the data provided to or obtained directly by an AI system from which an output result is produced;

Example – Prediction of risk of social exclusion and assessment of access to aid/subsidies
Input data is that which is entered into the system, once it has been trained, validated, tested and put into service. In the case of use, it would be all the information collected for the application process by the person responsible for the deployment, as well as reports that may be provided or requested from other entities (social protection, primary care, etc.), likewise, in the case of the public administration, the system could use as input data those that come from other sources already registered, such as data from the Treasury, Cadastre, etc.

3.13 Biometric identification

Biometric identification: the automated recognition of physical, physiological, behavioural or psychological human characteristics to determine the identity of a natural person by comparing their biometric data with the biometric data of people stored in a database.

Example – Biometric identification at work
The act of recognizing the biometric characteristics of employees, through cameras placed at the entrance of said facilities. In this context, this AI system is a biometric identification system, depending on the use it may or may not be considered high risk.

3.14 Biometric Verification

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

Example – Biometric identification only to verify the identity of a worker at work access
The automated comparison of the identified biometric data against the reference data of the company's database. In this context, this AI system is a biometric identification system but not high risk when used to only allow access to the company.

3.15 Biometric categorisation system

Biometric categorisation system: an AI system intended to include natural persons in specific categories based on their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons.

Example
An AI system categorizes website users and potential customers based on their behaviour on it, through an analysis of the keystroke.

3.16 Remote Biometric Identification System

Remote biometric identification system: an AI system aimed at identifying natural persons without their active participation and usually remotely by comparing their biometric data with those contained in a reference database;

In other words, the AI system aims to detect several people or their behaviour simultaneously, in order to considerably simplify the identification of people without their active participation. AI systems intended for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person they claim to be, as well as the identity of a natural person for the exclusive purpose of having access to a service, unlocking a device or having security access to a premises, are excluded.

3.17 Serious incident

Serious incident: an incident or malfunction of an AI system that, directly or indirectly, has any of the following consequences:

(a) the death of a person or serious damage to his or her health;

(b) a serious and irreversible disruption to the management or operation of critical infrastructure;

(c) failure to comply with obligations under Union law to protect fundamental rights;

(d) serious damage to property or the environment;

Example – Chronic Disease Management – Smart Insulin Pump
The AI system collects data regarding blood glucose concentration and together with other attributes stored in the patient's database (patient's physiology, history, activities, such as meals and physical activity) analyzes and determines the correct dose of insulin to be administered. Expanding on the example of the definition of withdrawal of the artificial intelligence system, in this scenario, a failure in the system could result in an administration of insulin due to excess or deficiency, if an incident were caused that causes death or serious damage to health, it would be clearly serious.

3.18 Real-world testing plan

Real-world testing plan: a document describing the objectives, methodology, geographical, population and temporal scope, monitoring, organisation and conduct of the real-world test.

3.19 Deep fake

Deep fake: Image, audio, or video content generated or manipulated by an AI that resembles real people, objects, places, entities, or events and that may mislead a person to think that they are authentic or true.

3.20 General Purpose AI Model

General-purpose AI model: an AI model trained on a large volume of data using large-scale self-monitoring, which has a considerable degree of generality and is capable of competently performing a wide variety of different tasks, regardless of how the model is introduced to the market, and which can be integrated into a variety of downstream systems or applications; except for AI models that are used for research, development, or prototyping activities before they are introduced to the market.

Requirement to be considered GPAI: its computational cost of training is greater than the order of >1023 $FLOPs$

Example
OpenAI's models such as: GPT-4, GPT-3; from Meta, the LLaMA family of models; Google's Gemini ultra or Gemini pro; from mistral: Mistral Large 2 or Mistral Small; Anthropic Claude 3 Opus or Claude 3 Haiku; among others. It must be distinguished from general-purpose AI systems, such as ChatGPT or Copilot.

3.21 Systemic Risk

Systemic risk: Some general-purpose AI models may present additional risk due to the high-impact capabilities they have. By having a significant impact on the Union market due to its scope or actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights or society as a whole, which may spread on a large scale along the entire value chain.

Requirement to be considered GPAI with systemic risk: its computational cost of training is higher than the order of $> 10^{25}$ $FLOPs$

3.22 Life cycle of an AI system

Life cycle of an AI system: a structured and well-defined sequence of the stages that the software goes through during its useful life, from the definition of the initial requirements (design inputs) to its retirement, including the design and development stages, validation and verification testing, deployment, operation and monitoring, continuous re-evaluation and validation.

4. Introduction to Technical Guides

This section provides a context for the preparation and objective of the technical guides, prepared within the framework of the Spanish AI sandbox pilot promoted by the Secretary of State for Digitalisation and Artificial Intelligence with the support of the European Commission.

The objective of the sandbox and all the materials developed and made available to the public is to help the Spanish business fabric to advance in AI regulatory compliance, providing support to companies for the commercialization of high-quality AI systems, increasing public confidence in the use of this technology.

4.1 The Spanish Sandbox IA pilot

The Spanish AI Sandbox pilot is a controlled test environment that **seeks to promote the responsible development of AI, validating the adequacy of high-risk systems to the requirements of the Regulation through conformity assessment simulations**. Its main objective is to clarify the obligations of the Regulation for startups and SMEs, validate the usefulness of technical guides and facilitate the transfer of knowledge to create solutions aligned with legal and ethical principles. In addition, it promotes reliable innovation, strengthens the supervisory capacity of the Spanish Agency for the Supervision of AI and allows the real impact of regulatory obligations to be assessed, contributing to European standardisation. Ultimately, it aspires to position Spain as a leader in responsible AI at a European and global level.

In November 2023, the Secretary of State for Digitalisation and AI, in close collaboration with the European Commission (DG CNECT), published Royal Decree 817/2023, which establishes the regulatory bases for the participation of companies in the AI sandbox. Subsequently, in December 2024, the official call was launched by resolution. In January 2025, the event to present the call was held.

After the evaluation of the 41 proposals submitted, 12 high-risk systems in different sectors were selected:

Illustration 1: Sandbox Participants

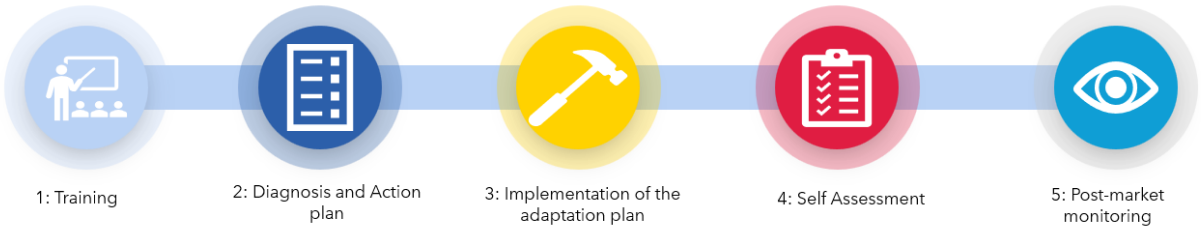
Participants

Sector	Description	System	Collaborators	Users
Access to services and assistance	**Intelligent transcription processing system for emergency communications** of the Galicia 112 Operations Centre	citic	CLUSTER TIC GALICIA, cinfo	axega
	AI system for **credit scoring, creditworthiness assessment and default risk analysis** of individuals based on their banking transactional data	DEDOMENA		BBVA ikualo
Biometrics	**BioSurveillance** – High-performance **video surveillance solution** based on facial recognition (using biometric data). It is specifically designed for the **simultaneous identification of individuals in crowded and highly dynamic environments**	herta		
	Veridas Age Verification – System for **verifying users' age on vending machines**, ensuring regulatory compliance in the sale of regulated products such as tobacco, as well as products subject to pending regulation, such as vaping products	VeriDas	GM	UAM
Employment	**Shakers AI Matchmaker –** AI-driven matching system that uses personalised recommendations to **connect freelance talent with business projects**	SHAKERS		BBVA
	Ranking of applicants via HyM (How You Match) – Assessment of suitability for the position through **compatibility scoring between candidates' CVs** and the requirements of job postings on InfoJob	Adevinta	Hirint.	SIETE ESTRELLAS SOCIALMENTE, Proselección, a1 SOLUCIONES
Critical infrastructures	GuardianMobility AI – Advanced real-time monitoring designed for the safety and optimization of critical transport infrastructures. Early detection of incidents and anomalies involving vehicles, crowds, and strategic spaces.	imotion. Analytics		
	AI-enhanced cybersecurity in Loradix – AI-driven cybersecurity for the control of external data flows to and from the electricity distribution telemanagement system.	LORADIX	GFT, S2 GRUPO	estabanell energía, aduriz energía, DISTRIBUCIÓN ELÉCTRICA CREVILLENT, TESELADOS RED, S.L.
Healthcare	CL@UDIA – A platform for the support, treatment, and prevention of sleep disorders, based on the collection of multimodal data acquired through wearable systems used by users in their home environment.	Bitbrain		
	Tucuvi Health Manager – Medical software that automates patient clinical monitoring via telephone calls handled by a conversational AI–based virtual assistant	tucuvi	indra, Google Cloud	
	MoGIA-MetCare: AI for Metabolic Disease Prevention – Integrating clinical data (anamnesis) with analytical and genetic biomarkers to deliver personalized risk assessment for metabolic diseases, including diabetes and obesity	MADEOFGENES	GENOMCORE	
Machinery	Operator Assistant for SOI Usage – A web application that uses a chatbot to answer questions based on a selected Standard Operating Instructions (SOI) document	AIRBUS	INDESIA, A:STACK LABS	

Prior to the start of the project, technical guides had been developed, precursors of these guides, with the aim of facilitating the understanding of the European Regulation on Artificial Intelligence and the obligations applicable to high-risk systems to participants in the sandbox. These guides are not binding or a substitute for regulations, but offer practical recommendations aligned with regulatory requirements.

In April 2025, the **kick-off** event was held in which the working mode was presented to the selected participants with the proposed work schedule and the main milestones to be achieved. To sum up, participation is structured in five phases:

Illustration 2: Sandbox Phases



To support the development of the sandbox activities, on June 10, 2025, the **group of 40 expert advisors** was appointed by Resolution. This group is made up of independent professionals of recognized prestige and technical experience in related fields of knowledge, with present or past responsibilities in the academic and university field, in collegiate institutions, associations of other types, or in the business sector. Its objective is to provide technical knowledge, support participants from their experience and prepare training material that can be used by Spanish companies in their regulatory adaptation initiatives.

4.2 Context of publication of the technical guides

The technical guides prepared within the framework of the Spanish AI Sandbox pilot have been developed thanks to the collaboration between the Secretary of State for Digitalisation and Artificial Intelligence as the promoter of the initiative and different actors: the participants, technical assistance, the group of expert advisors and various potential national competent authorities of the Regulation.

During their preparation and use, it has been observed that, during the process of developing common standards and specifications of the AI Act, **they are helping the participating companies to advance in their initiatives aimed at ensuring future regulatory compliance, as well as improving their internal quality and safety systems** in the development of AI.

That is why it has been estimated that the publication of this material could be of tremendous use to the Spanish business fabric, especially for SMEs and start-ups. As indicated on the back cover of each guide, **the guides are not binding and do not replace or develop the applicable regulations**, they simply **provide practical recommendations aligned with regulatory requirements pending the approval of harmonised rules of application for all member states**.

Below is a summary of the obligations and roles set out in the AI Act for providers and deployment managers that are covered in the technical guides:

Operator	Obligation	IA Act	Associated guide

HRIA Provider	Compliance with requirements section 2 of the Regulation	Art 16.a	15. Technical Documentation Guide 11. Cybersecurity Guide 7. Data and Data Governance Guide 5. Risk Management Guide 9. Accuracy Guide 10. Robustness Guide 8. Transparency Guide 6. Human Oversight Guide
HRIA Provider	Have a quality management system in place	Art 16.c	4. Quality Management Guide
HRIA Provider	Retain log files automatically generated by your systems	Art 16.e	12. Records Guide
HRIA Provider	Conformity assessment procedure	Art 16.f	3. Conformity assessment guide
HRIA Provider	Take necessary corrective action	Art 16.j	14. Serious Incident Reporting Guide
HRAI Providers	Incident Reporting	Art 73	14. Serious Incident Reporting Guide

Operator	Obligation	IA Act	Associated guide

HRIA Deployment Manager	Assign human oversight of the system to individuals with the necessary competence, training, and authority.	Art 26.2	6. Human Oversight Guide
HRIA Deployment Manager	Retain log files automatically generated by your systems	Art 26.6	12. Records Guide
HRIA Deployment Manager	Inform the supplier or distributor if they believe that the use of the system in accordance with their instructions may result in a risk to health, safety or fundamental rights**Error! Bookmark not defined.**, and suspend the use of the system if applicable	Art 26.5	14. Serious Incident Reporting Guide
HRIA Deployment Manager	Inform the supplier or distributor, the importer and the market surveillance authority of serious incidents.	Art 26.5	14. Serious Incident Reporting Guide

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