Guide 12. Automatically generated records and records files

European
Artificial Intelligence Act

12

Companies developing compliance with requirements

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 pilot for the regulatory AI Sandbox, through collaboration among participants, technical assistance providers, potential competent national authorities, and the sandbox's expert advisory group.

The aim of the guide **is to serve as an introductory support to the European Regulation on Artificial Intelligence and its applicable obligations.** Although it is not legally binding and does not replace or develop the applicable legislation, it provides practical recommendations aligned with regulatory requirements, pending the approval of the harmonised implementing standards for all Member States.

This document **is subject to an ongoing process of evaluation and review, with periodic updates** in line with the development of standards and the various guidelines published by the European Commission, and it will be updated once the Digital Omnibus amending the Artificial Intelligence Act is approved.

Among the relevant technical references currently under development and applicable are **ISO 15489-1:2016 "Information and documentation - Records management - Part 1: Concepts and principles"**, **ISO 31000:2018 "Risk management - Guidelines", ISO/IEC 23894 "Information technology - Artificial intelligence - Guidance on risk management"**, **ISO/IEC 42001 "Information technology - Artificial Intelligence - Management system", prEN 18229-1 "AI Trustworthiness Framework - Part 1: Logging, Transparency and Human Oversight"** and **prEN ISO/IEC 24970 "AI System Logging"**. These will serve as the foundation for establishing a common framework for the management, logging, transparency, and oversight of artificial intelligence systems, integrating the principles of records management, risk management, and governance management within the context of compliance with the European Regulation on Artificial Intelligence

Revision date: 10 December 2025

General content

Detailed Index

1. Preamble

1.1. Purpose of the document

This guide presents the **measures** that will help providers and those responsible for deploying AI systems to **comply with** the **requirements of the European Regulation on Artificial Intelligence (AI Act)** regarding the **generation and retention of records**, which all high-risk AI system (HRAIS) must incorporate.

The development of an adequate **record management system** not only will it make it possible to comply with the requirements of the European Regulation on Artificial Intelligence but also **facilitate** other tasks such as **transparency** and **accountability** or **research activities** and **test-driven development**. These benefits and some others will be discussed in more detail in section 5.

1.2. How to read this guide?

The structure of this guide presents a **first section** with the preamble to this guide.

A **second** introductory section where what a record is defined, and its main characteristics are mentioned.

In a **third section** focused on the European Regulation on Artificial Intelligence and the articles around records, a table is also included with each of these articles and their references from within the sections of this guide to facilitate their location.

The **fourth section** delves into records, including a description of the types of records, the aspects that each of them must contain, and the obligations of the actors involved in the preservation of records.

The **fifth section** describes the processes that must be addressed for the development of an adequate and complete management of records.

The **sixth section** covers the technical documentation related to records systems and the **seventh section** includes some issues to facilitate the self-assessment of AI systems.

Finally, the **eighth and ninth sections** include, respectively, a glossary of terms and references to norms and standards that have been consulted for the preparation of this guide.

1.3. Who is it for?

It is the responsibility of the providers and deployers of high-risk AI systems to implement appropriate measures to ensure the records retention and maintenance obligations mentioned in the European Regulation on Artificial Intelligence.

1.4. Use cases and examples throughout the guide

In order **to facilitate** the **understanding of the guide,** different examples **are incorporated in it** that aim to serve as **a reference** for the adequacy of the HRAIS for the **generation of records** in accordance with the requirements of the AI Act.

These examples are developed based on the **use cases** described in the **Cross-Cutting Information and Concepts Guide**.

Finally, it should be noted that whenever an example is given, it will be done in an illustrative way. Provider and deployer should consider implementing all measures outlined in this guide, as appropriate. Each AI system, following the guidelines in this guide, should identify and implement the most appropriate measures according to the characteristics of its AI system and its specific purpose. In addition, the examples presented are specific to the use cases.

This implies that proposals are specific to the models considered as examples, and not a general solution to other for other type of models, or even models of the same methodology. Each organization shall, in accordance with this guide, establish the appropriate measures for its type of AI system and its intended purpose.

The selected examples to be addressed in this guide are:

- **AI system for promotion**
- **AI system for insulin delivery**
- **AI system for biometric recognition in work attendance**

2. Introduction

2.1. What is a record?

In an AI system, a record is a file that stores information about the behaviour and performance of the system during training or production use. The record can include things such as information about system input data, predictions made by the system, and any errors or anomalies that occur during system execution.

The records are very important tools for the analysis and continuous improvement of the AI system. It allows 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 and take steps to correct them.

In addition, records are information assets that can act as evidence of AI system events, allow you to track the execution and behaviour of the system, and help ensure that the system operates as intended purpose.

2.2. What is a record management system?

In the context of AI, a record management system is a set of processes that are defined to collect, store, analyse, and manage the records generated by a AI system. It is critical for monitoring system performance, detecting issues, and improving AI model accuracy.

Additionally, it is important that the system meets data security and privacy requirements, as records may contain sensitive and confidential information.

In section 5 The processes that comprise a records management system will be analysed in detail; in summary these are:

- **Assessment** of the need for the creation of the records and their **design**.
- **Capture, storage and access control** over records guaranteeing their security.
- **Retention** and **deletion** of records.
- **Continuous monitoring and improvement** of the system.

2.3. What principles should we guarantee in the management of records?

In the management of records of AI systems it is important to try to guarantee a series of principles that help to generate functional, valid and reliable records:

- **Confidentiality**: records must protect the privacy and confidentiality of the recorded data, preventing its unauthorized disclosure or access.
- **Integrity**: records must be accurate and complete, without unauthorized changes, to ensure the reliability of the data recorded.

- **Availability:** Records should be available when needed, so they can be analysed, audited, or reviewed if needed.
- **Authenticity**: records must be authentic, i.e. they must be registered by the system legitimately and not tampered with by unauthorized users.
- **Accessibility and traceability**: records should be accessible and available for review and analysis, and should be accompanied by traceability information, so that the source and origin of the recorded information can be identified.
- **Accountability**: records should be the responsibility of the AI system owner and should be handled appropriately and securely.
- **Retention and deletion**: records must be retained for an appropriate period of time, and then securely deleted to ensure that personal data protection regulations are not violated.

2.4. What are the benefits of proper record management?

As mentioned above, the development of this guide is focused on **helping the reader comply with the requirements of the European Regulation on Artificial Intelligence**. In this sense, in addition to compliance with the provisions of said Regulation, it is considered relevant to highlight that **an adequate management of records** of our AI system can **provide a differential value** in different horizons since it can help **in elements such as:**

- Transparency and accountability.
- Decision-making processes.
- Business continuity in the event of a disaster or loss of information.
- Protecting the rights and obligations of organizations and individuals
- Protection and support in litigation.
- The protection of intellectual property.
- Evidence-based research and development activities.

3. European Regulation on Artificial Intelligence

The commissioning of high-risk AI systems should be subject to compliance with certain mandatory requirements, including the requirement of records. Those requirements aim to ensure that high-risk AI systems available in the Union or whose output outputs are used in the Union do not pose unacceptable risks to important public interests recognised and protected by Union law.

This section includes the articles referring to the generation of records of the Regulation 2024/1689 of the European Parliament and of the Council, of 13 June 2024 (European Regulation on Artificial Intelligence) and details in which sections of this guide the different elements of these articles are addressed.

3.1. Previous analysis and relationship of the articles

The obligations on the generation of records are mainly found in two articles of the European Regulation on Artificial Intelligence, Article 12 *"Record-keeping"* and Article 19 *"Automatically generated logs"*. In addition, the obligations of those responsible for deployment set out in section 3 of chapter III *"Obligations of providers and deployers of high-risk AI systems and other interested parties"*, article 26 *"Obligations of deployers of high-risk AI systems."*

Due to the nature and content of these articles, they will be dealt with, in the specific case of this guide, together. In this sense:

- **Article Record-keeping →** Establishes that HRAIS must incorporate the technical capabilities necessary for the automatic generation of records. In addition, it points out a series of conditions that these records must meet.
- **Article Automatically generated logs →** Indicates that HRAIS providers must retain the record files (referred to in the article "Record-keeping") automatically generated by the system, as long as such files are under their control.
- **Article Obligations of deployers of high-risk AI systems →** With regard to the retention of records (paragraph 6), it indicates that those responsible for the deployment of HRAIS must retain the record files (referred to in the article "Record-keeping") automatically generated by the system, as long as those files are under its control.

3.2. Content of the articles in the AI Act

AI Act

Art.12 – Record-keeping

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

2. In order to ensure a level of traceability of **the functioning of a high-risk AI system** that is appropriate to the intended purpose of the system, **logging capabilities** shall enable the recording of events relevant for:

(a) **identifying situations** that may result in the high-risk AI system presenting **a risk** within the meaning of Article 79(1) or in a **substantial modification;**

(b) **facilitating** the **post-market monitoring** referred to in **Article 72**; and

(c) **monitoring the operation** of high-risk AI systems referred to in Article 26(5).

3. For high-risk AI **systems** referred to in **point 1 (a), of Annex III**, the logging capabilities shall provide, **at a minimum**:

(a) **recording of the period of each use** of the system (start date and time and end date and time of each use);

(b) the **reference database** against which input data has been checked by the system;

(c) the **input data** for which the search has led to a match;

(d) the **identification** of the **natural persons involved** in the verification of the results, as referred to in Article 14(5).

AI Act

Art.19 - Automatically generated logs

1. **Providers** of high-risk AI systems **shall keep the logs** referred to in Article 12(1), **automatically generated** by their high-risk AI systems**, to the extent such logs are under their control.** Without prejudice to applicable Union or national law, the logs shall be kept for a **period appropriate** to the intended purpose of the high-risk AI system, **of at least six months**, unless provided otherwise in the applicable Union or national law, in particular in Union law on the protection of personal data.

2.Providers that are **financial institutions** subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain **the logs automatically generated** by their high-risk AI systems **as part of the documentation** kept under the relevant financial services law.

AI Act

Art.26.6 - Obligations of deployers of high-risk AI systems

Deployers of high-risk AI systems shall keep **the logs automatically generated** by that high-risk AI system **to the extent such logs are under their control**, for a period appropriate to the intended purpose of the high-risk AI system, **of at least six months**, unless provided otherwise in applicable Union or national law, in particular in Union law on the protection of personal data.

Deployers that are **financial institutions** subject to requirements regarding their internal governance, arrangements or processes under Union financial services law **shall maintain the logs as part of the documentation kept** pursuant to the relevant Union financial service law.

3.3. Correspondence of the article with the sections of the guide

The following table details the sections of this guide that address the different elements of the articles:

Article	AI Act requirement	Section
12.1	Recording files throughout the entire system lifecycle	Section 2, Section 4.2 and Section 5
12.2.a	Screening for HARIS that present a national risk	Section 5.1.1
12.2.b	Facilitation of post-market monitoring.	Section 5.1.2
12.2.c	HRAIS Operation Monitoring	Section 5.1.3
12.3.a	Records of the period of each use of the high-risk system in Annex III	Section 4.3
12.3.b	Database against which the high-risk system in Annex III has been checked	
12.3.c	Input data that have returned correspondence (high-risk Annex III systems)	
12.3.d	Natural persons involved in the verification of results (Annex III high-risk systems)	
19.1	Conservation of record providers	Section 3.1 and section 4.1
19.2	Conservation of record providers (financial institutions)	
26,6	Retention of records deployers	

4. Records: actors and content

4.1. Agents responsible for the records

The obligations associated with high-risk AI systems in relation to the retention of records, referred to in Article 12, fall on both the provider and the deployer of the high-risk system.

- If I am the **provider** or **deployer** of the high-risk AI system:
  a) I will have to take care of the **conservation** of the records generated by my system (see section 5.3) as long as these records are under my control.
  b) I must keep them for a **period** of at least **six months** unless otherwise provided for in applicable Union or national law, in particular Union law on the protection of personal data.
  c) If I am a **financial institution,** I will be required to keep the records as **part** of the **documentation** kept under the relevant financial services legislation.

In the section 3.2 are cited the articles of the Regulation specifying the obligations of the provider and deployer in relation to the requirements for records.

4.2. What information can a record generally contain?

The records must represent the **information** who has been identified as **Necessary** After the **Evaluation Process** (see section 5.1).To give a more detailed idea of the information that can usually be contained in a record of an AI system, the most frequent attributes are attached below:

a) A unique identifier for the record.
b) The identity of the user or system that logged the event.
c) A description of the contents of the record.
d) The structure of the record (e.g., its form and format).
e) The context and purpose in which the record is created, received, and used.
f) The actions and events throughout the existence of the record.
g) Date and time of each action performed in the system.
h) Identification of the AI model or algorithm used, including the version and configuration parameters used.
i) Identification of the input data used by the AI system.
j) Source of the input data used by the AI system.
k) The type of input data used by the AI system.
l) Outputs produced by the AI system, including the output of the model or algorithm and any additional information generated by the system.
m) Metrics for the quality of the results (e.g. accuracy).
n) Performance and capacity monitoring information, such as resource usage (CPU, memory, storage), response time, and error rate.
o) Security and privacy information, such as user authentication and authorization, data encryption, and detection of unauthorized access attempts.

p) System-generated alerts or notifications, such as warnings of input data errors or system failures.
q) Relationships with other records.
r) Information that we believe is necessary to fulfil the evidentiary function for which the record is designed (see section 5.1).
s) Other information necessary to retrieve and submit the record (e.g., storage information).

Example - Promotion AI system

Taking as an example the **promotion AI system** of employees, an example of a record that could be generated (in the section 5.1 It is analysed in detail when and why it will be interesting to generate a record) is one that collects the following information:

- Date and time of each action taken in the system, such as sending promotion requests or reviewing candidate profiles.
- Identification of the user or users who performed each action, as this would allow full traceability of actions in the system and early detection of any discriminatory conduct.
- Profile of the candidates evaluated for each position, including relevant information such as education, work experience, and skills required for the position.
- Results of each candidate assessment, including scores, comments and notes made by the assessors.
- Any actions taken in response to evaluations, such as hiring or promotion decisions, and the justification for such decisions.
- System-generated alerts or notifications in case of detection of discriminatory patterns, such as frequent promotion of candidates of a certain gender or ethnicity.

Example – AI system for insulin delivery

Taking as an example the **AI system for insulin delivery**, an example of a record that could be generate (in the section 5.1 is analysed in detail when and why we will be interested in generating a record) is one that collects the following information:

- Date and time of each insulin administration.
- Type and amount of insulin given.
- Blood glucose level before administration.
- Blood glucose level after administration.
- System-generated alerts or notifications in case of detection of abnormal or dangerous patterns, such as glucose levels that are too low or too high, or frequent insulin administrations in a short period of time.
- Interactions with other medications or medical treatments of the patient.
- Any other relevant events recorded by the system, such as changes in the insulin dose prescribed by the doctor or changes in the patient's diet.

4.3. What information should a record of a remote biometric identification system contain?

A remote biometric identification system is, according to the Regulation, *"an AI system intended to identify natural persons generally remotely, **without their active participation**, by comparing their biometric data with those contained in a reference data repository"*.

In this regard, in addition to the common elements of the records of a AI system, if the system uses remote biometric identification (AI systems listed in point 1(a) of Annex III) it must incorporate some specific elements, which are indicated in paragraph 3 of Article III.:

AI Act

Art.12.3 – Record-keeping

For high-risk AI systems referred to in point 1 (a) of Annex III, the logging capabilities shall provide, at a minimum:

(a) recording of the period of each use of the system (start date and time and end date and time of each use);

(b) the reference database against which input data has been checked by the system;

(c) the input data for which the search has led to a match;

(d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14(5) (which states the following For high-risk AI systems referred to **in point 1(a) of Annex III**, the measures referred to in paragraph 3 of this Article shall be such as to ensure that, in addition, no action or decision is taken by the deployer on the basis of the identification resulting from the system unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority. The requirement for a separate verification by at least two natural persons shall not apply to high-risk AI systems used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate.)

In this context, what should be done if a biometric system has been developed to make sure that this additional information is collected in the records.

Here's an example for a use case for a biometric recognition AI system in work attendance:

Example – AI system for biometric recognition in work attendance

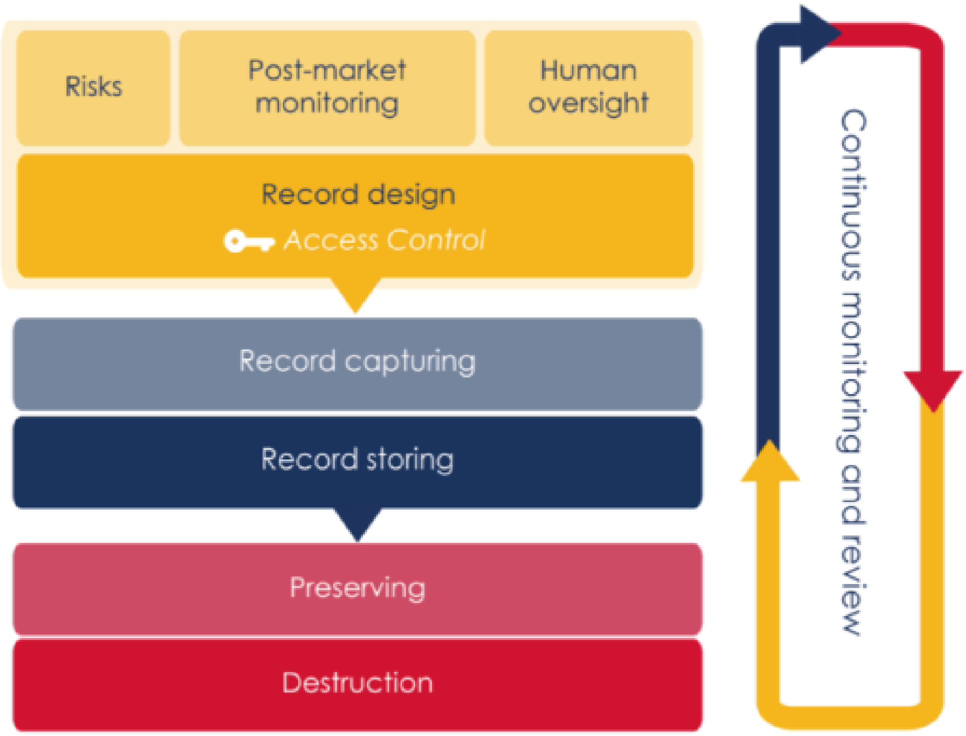
Taking as an example the **AI system for biometric recognition in work attendance,** an example of a record that might be generated (in the section 5.1 is analysed in detail when and why we will be interested in generating a record) is the one that collects the following information:

- Date and time of each identification made by the system (the start date and time and the end date and time of each use).
- The reference database against which the system has checked the input data.
- An image of the face that was analysed (the input data with which the search has returned a match).
- The identification of the two or more natural persons involved in the verification of the results.
- Identification results, including the person identified, whether a match was made, the confidence level of the identification, and any errors or anomalies detected.
- Information about the camera or device used to capture the facial image.
- Information about the location and context of the identification, such as where the system was used and the purpose of the identification (controlling the time worked).
- Any changes to the system, such as software or hardware updates, that may affect the behaviour of the AI system.

The information contained in these three examples on the aspects that a record should contain will also be mentioned in Chapter 5, as it is intended to place this design of records in the overall process of managing and maintaining records.

5. What elements should I implement and how should I do it to develop an adequate record management system?

This section describes the **processes** that must be addressed for the **development** of adequate and complete **records management**, from the assessment of the need for the creation of records to their disposition and disposal:



5.1. Evaluation and design of the records

What is it?

Evaluation is the **process of analysis** by which **the** need to generate records **and their** requirements. This will help determine what **information** should be **collected** in the records, thus establishing which records we should create and capture.

How should I approach it?

In general terms, this first phase consists of analysing and determining the need for the generation of the record, defining the specific objectives for the generation of the record and establishing its scope. In addition, in this phase the record will be designed, by identifying the fields and categories for the collection of information. This phase is crucial to establishing useful and effective records that meet the objectives of the records management system.

In this way, we can identify the following elements within the process of evaluating and creating the records:

- **Identifying the need**: The first step is identifying the need for the record. Why is the record needed? What are the goals of the record? It is important to clearly define the need to ensure that the record is useful and relevant.
- **Identification of the objectives**: Once the need for the record has been identified, it is necessary to define the specific objectives of the record. What is expected to be achieved with the record? What are the expected results? It is important that the objectives are clear and specific so that the effectiveness of the record can be assessed.
- **Defining the scope**: The next step is defining the scope of the record. What kind of information will be recorded? How long will the record be kept? It is important to establish the scope to avoid unnecessary or irrelevant information collection.
- **Design of the record**: Once the objectives and scope of the record have been defined, it is necessary to design the record. This involves defining the fields and categories that will be used to record the information, as well as the tools and software that will be used to capture, store, and access the information.
- **Identification of those responsible**: Finally, it is important to identify those responsible for the record. Who will be responsible for collecting and maintaining the information? Who will be responsible for ensuring the accuracy and integrity of the record? It is important to clearly define roles and responsibilities to ensure the effectiveness of the record.

Each organization will need to determine what its needs are for generating records. However, in the context of the European Regulation on Artificial Intelligence, there are several capabilities that records must bring to the AI system. Specifically, the text of the Regulation states the following:

AI Act

Art.12.2 - Records-keeping

In order to ensure a level of **traceability** of the functioning of a high-risk AI system that is appropriate to the **intended purpose of the system, logging capabilities** shall enable the recording of events relevant for:

(a) **identifying situations** that may result in the high-risk AI system presenting a **risk** within the meaning **of Article 79(1)** or in a substantial modification;

(b) **facilitating** the **post-market monitoring** referred to in Article 72; and

(c) **monitoring the operation** of high-risk AI systems referred to in Article 26(5).

In this sense, the evaluation process will consist of analysing these three elements and determining which records should be created and captured. Below, we go into more detail on each of these three areas.

5.1.1.Risk situations

Before this point can be addressed, the **measures** detailed in the **guide** describing the **risks management** system must **have been implemented** (see guide associated with the article on the risks management system).

Once the guide to the risks management system has been addressed, an **inventory** will be available with the with the risks dealing measures identified and analysed. As detailed in this guide, the main focus is on the management of those risks that may affect **people's health, safety or fundamental rights.**

The next step will be **to analyse and decide for each of these measures whether or not** it is considered **necessary to evidence a** certain event and consequently **generate a record with the requirements and contents that are established.** This decision and, where appropriate, the specification of the associated events and records must be incorporated, as appropriate, in documentary form as part of the measures for dealing with the associated risks.

A detailed example is provided below for the development of the different elements that make up the **evaluation and design phase of the records** in the context of the detection of situations that may result in the AI system presenting a risk to the **health, safety or fundamental rights of individuals.**

Example – AI system for biometric recognition in work attendance

In the example of the **AI system for biometric recognition in attendance at work**, the phases for the assessment of the need and design of the record focused on **ensuring a non-discriminatory process** in order to **mitigate risks** related to a possible violation of the **fundamental right to non-discrimination** They would focus on the following:

- **Identification of the need**: In this phase, the need to have records to guarantee a non-discriminatory process in the biometric recognition AI system used in work attendance would be identified. This need would be based on the concern to guarantee equal opportunities and avoid discrimination on any grounds, such as race, gender, sexual orientation, religion, etc.
- **Identification of the targets**: In this phase, the specific recording objectives for the biometric recognition AI system would be defined. For example, goals could be set such as: ensuring that the system does not discriminate based on race, gender, or other factors, ensuring that the accuracy of the system is equitable for all employees, etc.
- **Definition of the scope**: In this phase, the scope of the recording would be established. In the case of an AI system for biometric recognition in work attendance, the technical aspects of the system would be defined, such as the biometric recognition algorithms used, the way in which the biometric characteristics of employees are captured and processed, etc.

- **Design of the record**: In this phase, the record for the AI system for biometric recognition in work attendance would be designed. The fields and categories for information collection would be defined, the way in which the information would be stored, and the tools and software that would be used to capture, store, and access the information. Examples of data that could be collected include:
    - Date and time of each identification made by the system (the start date and time and the end date and time of each use).
    - The reference database against which the system has checked the input data.
    - An image of the face that was analysed (the input data with which the search has returned a match).
    - The identification of the two or more natural persons involved in the verification of the results.
    - Identification results, including the person identified, whether a match was made, the confidence level of the identification, and any errors or anomalies detected.
    - Information about the camera or device used to capture the facial image.
    - Information about the location and context of the identification, such as where the system was used and the purpose of the identification (controlling time worked).
    - Any changes to the system, such as software or hardware updates, that may affect the behaviour of the AI system.
- **Identification of those responsible**: Finally, those responsible for the management of the record would be identified. In this case, the responsibility for collecting and maintaining the information could be assigned to a specific team in charge of managing the records, and the responsibility for ensuring the accuracy and integrity of the record could be assigned to the developers of the biometric recognition AI system.

All this with the aim of guaranteeing the non-violation of the fundamental right to non-discrimination and therefore avoiding discrimination in the process of attendance at work through the use of the AI system with biometric recognition.

5.1.2.Post-market monitoring

As indicated in the previous section, the **measures** detailed in the **guide** describing the **post-market monitoring** system must **have been implemented** before this point can be addressed (see guide associated with the article in the post-market monitoring system).

Having addressed the guide describing the post-market monitoring system, the details of Article 72(2) are taken into account:

AI Act

Art.72.2 - Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems

The post-market monitoring system **shall actively and systematically collect, document and analyse relevant data** which may be provided by deployers or which may be collected through other sources on the performance of high-risk AI systems throughout their lifetime, and which allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Chapter III, Section 2. Where relevant, post-market monitoring shall include an analysis of the interaction with other AI systems. This obligation shall not cover sensitive operational data of deployers which are law enforcement authorities.

In this context, the first step to be taken is to determine what information and data from the AI system will need to be collected after it is commercialized. This will have been addressed when implementing the measures set out in the guidance describing the post-market **monitoring system**. Once this information has been defined, the necessary records must be designed to collect this information.

A detailed example is provided below for the development of the different elements that make up the **evaluation and design phase of the records** in the context of **data collection** to facilitate **post-market monitoring**. Always paying special attention to the detection of situations that may lead to the AI system presenting a risk to the **health, safety or fundamental rights of people.**

Example – Promotion AI system

In the example of the **AI system used for the evaluation and promotion of employees**, the phases for the assessment of the need and design of the record focused on **ensuring a non-discriminatory process** in order to **mitigate risks** related to a possible violation of the **fundamental right to non-discrimination** They would focus on the following:

- **Need Identification** : In this phase, the need to have a record to ensure that the AI system used for the evaluation and promotion of employees does not discriminate against any employee based on personal characteristics, such as age, gender, ethnic origin, sexual orientation, religion, among others, would be identified. This need would be based on the concern to ensure a fair and non-discriminatory process, which assesses the competencies and skills of employees in an objective manner.
- **Goals settings:** In this phase, the specific objectives of the record for the AI system used for the evaluation and promotion of employees would be defined. For example, objectives could be set such as: detecting possible biases in the AI system, ensuring that evaluation and promotion decisions are based only on

objective criteria and relevant to the position, monitoring the use of the AI system by the human resources team, among others.

- **Definition of the scope**: In this phase, the scope of the recording would be established. In the case of an AI system used for employee evaluation and promotion, the technical aspects of the system would be defined, such as evaluation criteria, metrics used to measure employee performance, AI model tuning parameters, among others.
- **Design of the record**: In this phase, the record would be designed for the AI system used for the evaluation and promotion of employees. The fields and categories for information collection would be defined, the way in which the information would be stored, and the tools and software that would be used to capture, store, and access the information. Examples of data that could be collected include:
    - Date and time of each action taken in the system, such as sending promotion requests or reviewing candidate profiles
    - Identification of the user or users who performed each action, as this would allow full traceability of the actions in the system and early detection of any discriminatory conduct
    - Profile of the candidates evaluated for each position, including relevant information such as education, work experience, and skills required for the position
    - Results of each candidate assessment, including scores, comments and notes made by the assessors.
    - Any actions taken in response to evaluations, such as hiring or promotion decisions, and the justification for such decisions.
    - System-generated alerts or notifications in case of detection of discriminatory patterns, such as frequent promotion of candidates of a certain gender or ethnicity.
- **Identification of those responsible**: Finally, those responsible for the management of the record would be identified. In this case, the responsibility for collecting and maintaining the information could be assigned to a specific team in charge of managing the records, and the responsibility for ensuring that the AI system used for the evaluation and promotion of employees is fair and non-discriminatory to the developers of the system.

All this with the aim of ensuring that the AI system used for the evaluation and promotion of employees is fair and does not discriminate against any employee based on personal characteristics.

5.1.3.Human oversight

As indicated in the previous sections, before this point can be addressed, the **measures** detailed in the **guide** describing the human oversight system must **have been implemented** (see guide associated with the article on the **human oversight**).

Once these measures have been implemented, the information that is considered necessary for the AI system to provide us with in order to meet the needs of human oversight will have been identified. More specifically, paragraph 5 of the article " *Obligations of deployers of high-risk AI systems*" refers to the need to **identify serious**

incidents in the AI system during its use in order to be able **to inform the provider and interrupt its operation.**

In this context, once the measures established in the *Human Oversight Guide* have been implemented, special attention should be paid to the information that the AI system should provide us. With this, as has been done in the previous sections, the necessary records must be designed to collect this information.

A detailed example is provided below for the development of the different elements that make up the **evaluation and design phase of the records** in the context of the **identification of serious incidents in the AI system** during its use. To do this, **inform the provider and interrupt its operation**. Always paying special attention to the detection of situations that may lead to the AI system presenting a risk to the **health, safety or fundamental rights of people.**

Example – Insulin Delivery AI System

In the example of the **AI system for intelligent insulin administration** for diabetic patients, the phases for the assessment of the need and design of the record where the purpose is **to detect any element that could put the patient's life at risk,** would focus on the following:

- **Identification of the need**: In this phase, the need to have a record that allows detecting any element that could put the life of the diabetic patient at risk in the use of the intelligent insulin delivery system would be identified. This need would be based on the concern to ensure safety and avoid possible serious complications in the patient's health, such as hypoglycemia or hyperglycemia.
- **Identification of the targets**: In this phase, the specific objectives of the record for the AI system for intelligent insulin delivery would be defined. For example, goals could be set such as: detecting any significant changes in the patient's glucose levels, preventing possible episodes of hypoglycemia or hyperglycemia, monitoring the patient's physical activity, etc.
- **Definition of the scope**: In this phase, the scope of the recording would be established. In the case of an intelligent insulin delivery system for diabetic patients, the technical aspects of the system would be defined, such as how insulin is measured and administered, how the patient's glucose levels are captured and processed, etc.
- **Design of the record**: In this phase, the record would be designed for the intelligent insulin delivery AI system. The fields and categories for information collection would be defined, the way in which the information would be stored, and the tools and software that would be used to capture, store, and access the information. Examples of data that could be collected include:
    - Date and time of each insulin administration
    - Type and amount of insulin given
    - Blood glucose level before administration
    - Blood glucose level after administration
    - System-generated alerts or notifications in case of detection of abnormal or dangerous patterns, such as glucose levels that are too low or too high, or frequent insulin administrations in a short period of time
    - Interactions with other medications or the patient's medical treatments

  - Any other relevant events recorded by the system, such as changes in the insulin dose prescribed by the doctor or changes in the patient's diet
- **Identification of those responsible**: Finally, those responsible for the management of the record would be identified. In this case, the responsibility for collecting and maintaining the information could be assigned to a specific team tasked with managing the records, and the responsibility for ensuring the accuracy and integrity of the record could be assigned to the developers of the intelligent insulin delivery AI system.

All this with the aim of guaranteeing safety and avoiding possible serious complications in the health of the diabetic patient through the use of the AI system for intelligent insulin administration.

Finally, this entire process of evaluation and design of the records must be addressed on a recurring basis, with the periodicity that we consider appropriate, depending on the frequency of updating or variation of the elements mentioned. For example, if there is a change in the context of the AI system, this will affect the risks analysis (see the guide for the risks management system article) and therefore need to be re-evaluated for new requirements for records.

5.2. Capture, storage, and access control

What is it?

It is the process of **capturing**, **storing** and **preserving** the **records defined** in the previous phase, **guaranteeing their protection** against unauthorised access, unwanted modifications, loss or destruction.

How should I approach it?

What must be done at this stage is to keep the records in such a way that they can be guaranteed against unauthorized access, unwanted modification, loss or destruction. To achieve this goal, we must:

a) Collect the information in the records according to the criteria established in the design phase (this will depend on the nature of the system, where it is implemented, the programming language, etc.).
b) Select the appropriate storage media and protective materials (e.g., instead of storing all records information on a single server, have redundant servers).
c) Implement appropriate cybersecurity and access control measures to ensure the security of records (see Cybersecurity guide).
d) Develop and define roles and responsibilities on the management of records.
e) Ensure adequate training and training of personnel involved in the management of records (for example, by defining mandatory courses for such personnel, as they must know the selected storage media, the cybersecurity measures that apply to them and the access control measures).
f) Consider other applicable regulations or laws such as the Data Protection Regulation (GDPR).

g) Regularly monitor and review storage media and the cybersecurity and access control measures in place (e.g., defining review periods and assigning a person responsible for ensuring that these reviews are carried out).

The records must include the appropriate storage and access control information to ensure the location and monitoring of the security of the records (for example, identification of the user who has accessed, level of permission held, geographical location from which it has been accessed, and date and time of access).

In addition, records systems must be designed to facilitate the use of records while they are kept, we must not only be concerned with collecting and storing records but also with designing the system so that they are accessible and usable. To do this, for example, copies can be created in an alternative location for access, so that the integrity and security of the records in their main storage place is not risked.

5.3. Retention and deletion of records

What is it?

It is the procedure by which the needs for **the conservation and destruction** of the records created, captured and stored must be established and collected.

How should I approach it?

When establishing the processes for retaining and deleting records, it should be taken into account that these will be determined fundamentally by two factors:

a) On the one hand, the need to preserve the records identified by it owners in the evaluation process, for example, in the scenario described in the section 5.1.1 records are available to ensure a non-discriminatory process in order to mitigate risks related to a possible violation of the fundamental right to non-discrimination. This record should be kept for as long as necessary to ensure this process, it may be necessary to analyse at any given time some decisions that the system may have made.
b) Second, any applicable regulatory or regulatory requirements should be considered, for example, data protection law or GDPR if our records include personal data.

The record destruction is a process that must always be authorized and documented and must be carried out in compliance with the security and access measures implemented. In addition, records involved in some type of legal process cannot be destroyed until their deletion is authorized.

5.4. Monitoring and continuous improvement

Its purpose is to ensure and improve the quality and effectiveness of the records management system. It is essential to develop a follow-up and establish certain periods for reviewing and updating the record management system. The following phases can be differentiated as part of this process:

- **Monitoring and identifying potential errors**: The first step is identifying potential errors that may be affecting the system. This can include errors in the recorded data, performance issues, security issues, among others.
- **Analysis of the recorded data:** Once these errors have been identified, it is necessary to analyse the recorded data to determine their cause. This may involve reviewing the records to find patterns or correlations between the data.
- **Implementation of improvements:** Once the causes of errors have been identified, it is necessary to implement improvements to the system to correct them. This may include updating software, improving data recording procedures, or training staff.
- **Evaluation of improvements:** After implementing the improvements, it is necessary to evaluate their effectiveness in solving the problems identified. This may involve comparing the data before and after improvements to determine if there has been an improvement in the system.
- **Continuous improvement cycle:** Finally, it is important to establish a continuous improvement cycle to keep the system up to date and continuously improve its performance. This involves repeating the previous steps to identify new potential errors and improve the system continuously.

In short, for the proper implementation of monitoring and continuous improvement in a records management system, we must pay special attention to the identification of possible errors, analyse the recorded data, implement improvements and evaluate its effectiveness to keep the system updated and improve its performance continuously.

5.5. Who should be responsible for managing the records?

Responsibilities and authorizations for the management of records must be established, considering all the processes of design, capture, storage, access controls, and retention and disposal. Responsibilities should be assigned to all personnel involved in any of these processes and should be reflected and documented in job descriptions and similar statements, where appropriate. In addition, the responsibilities assigned should be well documented and reflected in the document developed to reflect the process of managing the records.

Example - Promotion AI system

The following is an example of a possible distribution of responsibilities in an organization:

a) A person in charge of carrying out the evaluation processes is assigned to identify the needs for generating records (for example, it can be the person responsible for the AI system).
b) A person in charge of designing the records is assigned, depending on the requirements of the evaluation process (for example, this may be the same person as the person in charge of the evaluation).
c) A person in charge of the process of capturing the records is assigned (for example, we can assign this task to an independent professional outside the development of the AI system or its administration).

d) A person is assigned to ensure the continuous and reliable operation of the records systems under his or her control and to ensure that all documentation of the records management systems is complete and up-to-date (e.g. the system administrator).
e) A person in charge of managing the storage of the records is assigned (for example, this role can also be held by the system administrator).
f) A person is assigned to ensure the security of the records by implementing cybersecurity and access control measures (for example, this role could be held by a professional from the information security office).
g) A person is assigned to ensure the adequate training and qualification of the personnel involved in the management of the records (for example, this role could be held jointly by the professionals of the two previous points).
h) A person is assigned to be responsible for the retention and deletion processes of the records (for example, the person responsible for the evaluation could be responsible for defining the retention and deletion periods and the person responsible for capturing the records could be responsible for their execution).
i) A person responsible for ensuring the proper functioning of the records management system is assigned, supervising the proper execution of the tasks assigned in the previous sections (for example, a professional from the management of the organization).

5.6. Entities subject to sectoral legislation

AI systems providers that are **financial institutions** subject to requirements relating to their internal governance systems or processes under Union financial services law **shall maintain the record files automatically generated** by their high-risk AI systems **as part of the documentation** preserved.

6. Technical documentation

The obligation to maintain records in accordance with Articles 12 and 19 of the regulation has a cross-cutting nature, as the recording mechanisms must be integrated into multiple phases of the AI system's lifecycle – from development and testing to operation and post-market monitoring. Consequently, it could be considered that each technical section of Annex IV documenting processes, measures, or controls should include its own subsection on record-keeping (for example, recording design activities, risk management, or human oversight). However, the only points in Annex IV that are directly and explicitly related to the obligation of maintaining records are the following:

- 2(g) – The validation and testing procedures used, including test log files and test reports dated and signed by the responsible persons.
- 9 – The detailed description of the system established to assess the performance of the AI system in the post-market phase, including the post-market monitoring plan.

These two points alone could be considered sufficient to cover the essential documentary requirements of the regulation regarding record-keeping, as they encompass both the generation and preservation of logs during development and their maintenance during the operational phase. However, it is considered good practice to expand the documentation by also including and justifying the following complementary aspects:

a) The evaluation process and design of the records addressed, detailing the elements analysed, the need identified, the objectives, the scope, the details of the design and the persons responsible identified.
b) The process of capturing records developed, identifying all the relevant information of the process.
c) The details of the storage media where the records will be saved and retained.
d) The security, cybersecurity, and access control measures implemented to ensure the security of the records.
e) The roles and responsibilities defined and established on the records management processes, identifying the training and capacity building of each of the responsible parties if necessary.
f) The established periods of review and supervision of the storage media and the cybersecurity and access control measures implemented.
g) The retention needs of the records and the retention periods established.
h) Applicable rules or regulations (e.g., data retention law or GDPR).

This documentation must be disseminated and known by all the actors involved and must be reviewed periodically to ensure that all updates or modifications that the process of managing the records have undergone are included.

7. Self-assessment questionnaire

To carry out a self-assessment of compliance with the requirements of the European Regulation on Artificial Intelligence referred to in this guide, a global self-assessment questionnaire has been generated with a series of questions with the key points to be taken into account with respect to the obligations dictated by the articles of the AI Act mentioned in this guide.

It will be necessary to refer to this document in order to carry out the section of the self-assessment questionnaire corresponding to this guide.

8. Annexes

8.1. Annex A – Glossary of Terms

This guide has been developed with an approach that tries to explain each concept present in the guide when it is exposed, however, certain specific terms have been collected in this section as additional clarification:

1. **Access to the record:** right, opportune, meant to find, use or retrieve information.
2. **Agent:** Individual, work group, or organization responsible for or involved in the processes of creating, capturing, and/or managing records.
3. **Company classification system:** a tool for linking records to the context of their creation.
4. **Classification:** systematic identification and/or arrangement of business activities and/or records into categories according to logically structured conventions, methods and rules of procedure.
5. **Conversion:** The process of changing records from one format to another.
6. **Destruction:** The process of deleting or deleting a record, beyond any possible reconstruction.
7. **Disposition:** A range of processes associated with implementing records retention, destruction, or transfer decisions documented in disposition authorities or other instruments.
8. **Disposition Authority:** An instrument that defines the disposition of authorized actions for specified records.
9. **Evidence:** Documentation of a transaction.
10. **Function:** Group of activities that fulfil the main responsibilities to achieve the strategic objectives of a business entity.
11. **Migration:** The process of moving records from one hardware or software configuration to another without changing the format.
12. **Records(s):** Information created, received, and held as evidence and as an asset by an organization or person, in compliance with legal obligations, or in the business transaction.
13. **Management of records:** field of management responsible for the efficient and systematic control of the creation, reception, maintenance, use and disposition of records, including the processes of capturing and maintaining evidence of business activities and information about them and transactions in the form of records.
14. **System of records:** An information system that captures, manages, and provides access to records over time.
15. **Transaction:** The smallest unit of a Work Process consisting of an exchange between two or more participants or systems.
16. **Work process:** One or more sequences of actions necessary to produce a result that complies with the rules of governance.

9. References, Standards & Norms

For the development of this guide, the following norms and standards have been consulted and used:

- ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles.
- ISO 31000:2018 - Risk management – Guidelines.
- ISO/IEC 23894 - Information technology – Artificial intelligence – Guidance on risk management.
- ISO/IEC 42001 Information technology – Artificial intelligence – Management system.
- prEN 18229-1 AI trustworthiness framework – Part 1: Logging, transparency and human oversight
- prEN ISO/IEC 24970 AI System Logging

In addition, other norms and standards have been consulted on an ancillary basis, such as:

- ISO/IEC 27001:2022 - Information security, cybersecurity, and privacy protection – Information security management systems – Requirements.
- ISO/IEC 22989:2022 - Information technology – Artificial intelligence – Artificial intelligence concepts and terminology.
- ISO/IEC 23053:2022 - Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).
- ISO/IEC 5259-1 - Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 1: Overview, terminology, and examples.
- ISO/IEC TR 24027:2021, Information technology – Artificial intelligence (AI) – Bias in AI systems and AI aided decision making.
- ISO/IEC AWI TS 12791 - Information technology – Artificial intelligence – Treatment of unwanted bias in classification and regression machine learning tasks.
- NIST - AI Risk Management Framework.

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).

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