agencia
española
protección
datos

GENERAL POLICY FOR THE USE OF GENERATIVE AI IN ADMINISTRATIVE PROCESSES OF THE AEPD

27th November 2025 version

Table of Contents

Internal version 1

1. INTRODUCTION 4

2. OBJECTIVES OF THE IMPLEMENTATION OF THE GENAI IN THE PROCESSES OF THE AEPD 5

3. USE CASES IN THE ADMINISTRATIVE FIELD OF THE AEPD 5

4. ANALYSIS OF THE RISKS POSED BY THE GENAI 11

5. GENAI GOVERNANCE, POLICY AND MANAGEMENT 13

A) Internal governance 13

B) POLICIES 14

GenAI SOLUTION TYPE SELECTION POLICY 14

POLICY ON THE TREATMENT OF PERSONAL AND SENSITIVE OR CONFIDENTIAL INFORMATION 16

USE CASE DESIGN POLICY 17

AVAILABILITY AND RESILIENCY POLICY 18

TRANSPARENCY POLICY REGARDING THE USE OF GenAI 18

EXPLAINABILITY POLICY 19

POLICY REGARDING AUTOMATED DECISIONS AND THEIR MONITORING 19

POLICIES REGARDING THE PROTECTION OF FUNDAMENTAL RIGHTS AND PROCESSING OF PERSONAL DATA 20

CYBERSECURITY POLICY 21

HIRING POLICY 22

HUMAN RESOURCES POLICY IN RELATION TO THE GenAI 23

EMPLOYEE USAGE POLICY 24

OVERSIGHT POLICY FOR THIS POLICY 24

C) PROCEDURES 25

PROCEDURE FOR DRAFTING, APPROVING AND REVISING THIS GENERAL POLICY 25

HOW TO INCORPORATE A USE CASE 25

PROCEDURE FOR DESIGNING AND DEPLOYING A USE CASE 26

INCIDENT MANAGEMENT PROCEDURE 27

PROCEDURES FOR MONITORING THIS POLICY 28

6. CONCLUSIONS 29

7. REFERENCES 29

1. INTRODUCTION

As set out in the 2020-2025 Strategic Plan, the Spanish Data Protection Agency (AEPD) is committed to an AI-first policy, promoting the safe and responsible use of artificial intelligence in all areas where it is possible. The Agency shares the conviction that the incorporation of AI – and in particular generative artificial intelligence (hereinafter GenAI) – should be integrated as a normal process in the functioning of public administrations, as in other sectors of society. The objective is to achieve maximum efficiency and quality in the exercise of public functions, taking advantage of the capabilities that AI offers to improve processes and services, in compliance with the constitutional principle of effectiveness and the constitutional and legal mandates of efficiency and continuous improvement that guide administrative action.

The AEPD aspires to become an institutional benchmark in the use of intelligent systems applied to public administration, demonstrating that technological innovation can coexist with regulatory compliance, the protection of fundamental rights and the promotion of a modern organisational culture, open to change and prepared for the challenges of the digital future.

This document, in its first version, establishes the bases for an institutional policy of implementation, responsible use in the use of Generative Artificial Intelligence services in the administrative processes of the AEPD, and whether or not they are processes that involve, or not, personal data (processing), which guides their progressive and effective deployment. This policy is approved in the exercise of the powers of self-organisation and within the framework of the independence of the AEPD, and forms part of the Agency's Information Policy[1].

The general policy described in this document promotes, within the Agency, transparency, security and trust in the implementation of artificial intelligence by the AEPD, with appropriate guarantees in the processing of personal and non-personal data or a combination of both, and with a comprehensive and law-abiding approach to the use of AI. This is an internal policy, applicable exclusively to the AEPD, which is not interpretative in nature with respect to the Artificial Intelligence Regulation[2] or other European or national regulations. This policy does not accredit, presuppose or develop obligations arising from the Artificial Intelligence Regulation, and is expressly outside any function of analysis, application or interpretation of said Regulation, including that relating to the identification of prohibited or high-risk systems[3] and the obligations linked to them. The scope of this Policy is therefore limited to the use of GenAI in the administrative processes of the AEPD, and in no case can it be considered a verification, evaluation, certification or indirect form of application of the Artificial Intelligence Regulation.

[1] The assignment of responsibilities should not be confused with the figure of the controller as defined in the GDPR.

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, to the extent applicable to deployed AI systems and general-purpose models used.

[3] References to "high risk" or similar that may appear in this Policy are in response to the common use of this expression in areas of data protection, risk management or organisational analysis. They do not imply in any case they are related to the category of high-risk systems defined by the Artificial Intelligence Regulation

2. OBJECTIVES OF THE IMPLEMENTATION OF THE GenAI IN THE PROCESSES OF THE AEPD

The objectives of the AEPD in relation to the deployment of the GenAI system in the AEPD processes are:

- **Increasing the effectiveness, efficiency and quality of the AEPD's processes through innovation:** An increase that does not have to be punctual but must be sustained and at the same time that new GenAI technologies are being deployed.

- **Protect fundamental rights**: Protection of the rights and freedoms of both employees and citizens in general, in particular in relation to the protection of personal data, and beyond strict regulatory compliance, based on the principle of proactive responsibility.

- **Protect the sensitive or confidential information of the AEPD:** For these purposes, sensitive or confidential information will be understood as any data that, if disclosed or accessed without authorisation, may pose a risk or damage to natural and legal persons, or to the objectives of the organisation.

- **Guarantee health and safety at work:** The deployment of GenAI systems can be carried out by implementing measures that directly benefit and protect the worker, avoiding risks of objectification, uncertainty in the face of new scenarios or other cognitive risks.

- **Ensuring process continuity**: Ensuring that the technological redefinition of processes maintains their availability and resilience.

- **Control operational and financial costs:** GenAI is an investment in the organization and the solutions that are deployed have to consider that it is not only a matter of savings but also of strategic efficiency, so that the economic factors to be scalable and maintainable.

- **Strengthen citizens' trust in the AEPD;** Guaranteeing coherence in the application of criteria and response to citizens, and accompanying the increase in efficiency with greater transparency, explainability and traceability in the actions carried out.

3. USE CASES IN THE ADMINISTRATIVE FIELD OF THE AEPD

Within the framework of this policy, scenarios are identified where GenAI systems add value and efficiency to the administrative processes developed by the AEPD. Each scenario is called a "use case" and involves implementing one or more AI systems in an AEPD process.

There will be processes that do not process personal data, and others that do process personal data (data processing according to the GDPR). In any case, each use case requires analyzing the impact that the GenAI system(s) has on the entire process, including the interaction with other systems that are not based on GenAI[4] , the human and material resources, and the organizational procedures of those processes.

The identified use cases show the main applications of the GenAI in the internal processes of the AEPD, common in public administrations. They range from support tasks for institutional communication, document writing, office automation or the preparation of training materials, to the generation of reports, summaries or translations of publicly accessible documents. Applications aimed at improving internal management are also contemplated, such as regulatory assistants, tools to support the processing of procedures or intelligent systems for monitoring the strategic plan. Similar use cases[5] may present significantly less risk or impact when they do not incorporate information with personal data, sensitive or confidential information.

The following table of identified use cases is not exhaustive or binding, but exemplifying, and will be updated in accordance with technological developments, applicable regulations and the organisational needs of the Agency.

It should be reiterated that this policy does not evaluate or classify use cases in terms of the Artificial Intelligence Regulation. However, and in any case, it is considered that none of the use cases can fit into the category of high-risk systems - nor, obviously, prohibited - defined by said Regulation. As a matter of caution, if at a later stage of development or deployment it is found that a use case could be included in any of the cases regulated by the Artificial Intelligence Regulation, the legal regime provided for in said instrument would be applicable in its entirety.

[4] Such as data collection, processing, transmission, storage or even decision support systems not based on GENAI systems.

[5] It is important not to confuse the risk that may exist in process (or processing when there is personal data) with the risk of an AI system. In many use cases of different risks, the same system is considered. Nor should we confuse the risk that the use of an AI system can pose to an organization (such as reputational risk) with the risk classification that an AI system has according to Regulation (EU) 2024/1689.

Use Cases	Description
Structuring, management or summarization of general and open documents (public documents)	Application of intelligent models to summarize, extract key information and transform public or non-confidential documents into structured formats that facilitate their analysis or reuse. Classification or automated analysis versions may be generated for study or dissemination purposes, guaranteeing in any case the anonymization and exclusion of personal data.
Translation of public documents	Facilitate the translation of public documents in different languages. It allows documents written in foreign languages (e.g. resolutions of European authorities) to be translated into Spanish, or vice versa, adapting the style of the translation according to the target audience.
Generation of institutional communication content	Comprehensive assistance in the production and review of institutional communication materials.
Generation of diagrams, concept maps and infographics for communication	Creation of diagrams, concept maps and explanatory infographics based on public information or open sources, to support the understanding and dissemination of content.
Generation of interactive multimedia and communication material and content	Development of interactive multimedia content for public education and dissemination, as well as automatic composition of music or ambient sound to accompany videos or institutional or promotional public events.
Generation of audios or videos from content and open documentation	Generation of voiceovers or synthetic videos, obtained exclusively from public or non-confidential documentation and without personal data, applicable to audio guides, telephone services or accessible materials.
Preparation of informative or training content	Support in the creation of awareness-raising and internal or external training materials on data protection, accessible and adapted to different profiles.
Identifying trends or patterns from open sources	Identification of trends or patterns through the automated analysis of open information to support decision-making.

Preparation of graphs, tables and reports from publicly accessible or non-confidential information	Automatic preparation of graphs, tables and financial or budgetary reports based on publicly accessible or non-confidential data, guaranteeing the exclusion of personal or sensitive information.
Assistance in the approach and general preparation of arguments, legal and technical studies	Use of generative AI systems for the analysis and comparison of legal, doctrinal or technical sources of a public or non-confidential nature, in order to develop argumentative frameworks, comparative studies, technical notes or interpretative hypotheses. These tools support the preparation of legal strategies or approaches without replacing professional valuation or involving automated decision-making. They can also be used for the exploratory and systematic analysis of legal or open sources, the comparison of regulatory or doctrinal frameworks, and the preparation of general studies that do not involve confidential information or personal data.
Assistance in the initial drafting of general and isolated elements whose ideas can then be incorporated into resolutions, reports or technical guides	Use of generative AI systems for the analysis and comparison of legal, doctrinal or technical sources of a public or non-confidential nature, in order to develop argumentative frameworks, comparative studies, technical notes or interpretative hypotheses. These tools support the preparation of legal strategies or approaches without replacing professional valuation or involving automated decision-making. They can also be used for the exploratory and systematic analysis of legal or open sources, the comparison of regulatory or doctrinal frameworks, and the preparation of general studies that do not involve confidential information or personal data.
Assistance with system development and configuration tasks	AI has become a key tool for technical tasks such as scripting, generating SQL queries, building regular expressions, and resolving doubts about specific software. It makes much of the work easier, allowing users to focus on checking and fine-tuning instead of starting from scratch. This is especially useful in environments where multiple technologies and advanced system configurations are handled.

Internal normative or doctrinal assistant	Development of internal virtual assistants that facilitate the rapid consultation of legislation, resolutions, legal reports, interpretative criteria of the Agency, etc., improving access to organisational knowledge. They can be used as support for enforcement, for the different phases of processing requests for approval of codes of conduct and those of requests for international transfer agreements, or for the preparation of anonymized summaries to support the dissemination of content, among others.
Transcription of audio and video from open sources without sensitive information	Transcription of media content from open or non-confidential sources for incorporation into different workflows or studies. It may contain personal data.
Audio and video transcription containing internal, private or confidential information, where applicable from meetings and support for the generation of minutes	Transcription of internal meetings, where appropriate to support the generation of minutes. As well as private audios of interviews or interventions made by the Agency's staff in acts or events and preparation of a summary of the resulting text.
Structuring, management or summaries of internal administrative documents or with personal data	Application of intelligent models to summarize, extract key information and convert internal administrative documents into standardized structures that improve their automated processing or analysis. In such cases, full or partial anonymisation of personal data should be applied and processing should be limited to secure and authorised environments, e.g. to prepare anonymised versions for transparency queries or internal reporting.
Writing drafts, letters, emails or internal notes with an institutional tone	Use of intelligent systems to prepare initial proposals for response to citizens or organizations, or written ones, speeding up processing times and guaranteeing coherence in institutional messages.
Generation of draft responses to queries for citizen service, DPO and youth channels.	The use of RAGs and well-tuned systems will allow access to updated information in real time on all the material produced by the AEPD to produce draft responses to specific queries from the citizen service channels, DPO channel and youth channel.

Classification and summary of complaints, queries and other entries.	Application of natural language processing (NLP) models to facilitate the initial processing of the information that reaches the Agency, allowing its categorization, indexing and preliminary analysis.
Support in the analysis of DPIA (Data Protection Impact Assessment)	Use of expert models to carry out an initial review or documentary support in impact evaluation reports, providing templates, common criteria or analysis guides.
Intelligent management of the strategic plan	The automation of the management of the strategic plan facilitates the real-time monitoring of the indicators related to the fulfilment of objectives and results. It allows the chosen methodology to be automated, optimises the execution of the strategy and allows decision-making based on real-time data. Data analysis and visualization of results for monitoring plans and indicators.
Assistance in the drafting of resolutions, reports or technical guides.	Use of generative AI tools to support the initial preparation of drafts of normative and doctrinal documents, facilitating the structuring of content and increasing efficiency in the production of documents related to specific cases.
Smart alert systems (prioritization of complaints, notifications and other inputs)	Development of AI systems that allow detecting and prioritising complaints, data breaches or sensitive communications, including automatic alerts for high-impact cases, vulnerable groups or situations that require priority attention at the discretion of the Agency, thus allowing agile and focused management.
Support for the processing of files and notifications of data breaches	The processing of files and/or notifications of personal data breaches are manual processes assisted by various corporate tools. GenAI makes it possible to speed up tasks, from the initial classification of entries by record, their categorization and extraction of structured information, to the preparation of summaries and drafts.

The use cases proposed do not exhaust the potential of the application of these technologies in the organization, which may be progressively expanded and will be incorporated into this policy once they are identified.

Before its implementation, each use case must be developed and analysed with the following criteria in an Annex to this general policy:

- Extended description.

- Division/Sub-directorate responsible.
- Estimated overall impact on the objectives of the AEPD.
- Recommended system type.
- Risks due to requirements or implications.
- Specific observations/obligations.

4. ANALYSIS OF THE RISKS POSED BY THE GenAI

The implementation of generative artificial intelligence in administrative processes, in particular due to its novelty, requires an analysis of the risks that must be identified and properly managed for each use case (or groups of use cases).

The risks have been managed according to how they may compromise the different objectives of the AEPD in relation to the deployment of the GenAI system in the AEPD's processes, among which is, as a priority, the protection of the rights and freedoms of citizens. The specific threats that involve the inclusion of GenAI systems in AEPD processes and that put the objectives at risk are identified below (they are developed in an Annex document), without prejudice to the particular risks that must be analysed in each specific process or processing in which the different use cases are applied.

Objectives of the AEPD	Threat Groups
Increasing the efficiency of AEPD processes through innovation	• Inefficiency of AI systems • Infrastructure insecurity and lack of process continuity • Wrong, irresponsible, or harmful human interaction with AI
Protecting fundamental rights	• Inefficiency of AI systems • Bias and discrimination • Impacts on rights and freedoms in relation to data protection: LIINE4DU • Infrastructure insecurity and lack of process continuity • Disclosure of Non-Personal Information • Wrong, irresponsible, or harmful human interaction with AI
Protect the sensitive or confidential information of the AEPD	• Infrastructure insecurity and lack of process continuity • Disclosure of Non-Personal Information • Wrong, irresponsible, or harmful human interaction with AI
Ensuring health and safety at work	• Impacts on rights and freedoms in relation to data protection. • Wrong, irresponsible, or harmful human interaction with AI • Impact on employee rights.
Ensure process continuity	• Infrastructure insecurity and lack of process continuity • Lack of governance and loss of institutional integrity
Control operational and financial costs	• Lack of governance and loss of institutional integrity
Strengthening citizens' trust in the AEPD	• Inefficiency of AI systems • Bias and discrimination • Impacts on rights and freedoms in relation to data protection. • Infrastructure insecurity and lack of process continuity • Lack of transparency and explainability of actions based on GenAI • Lack of coherence in similar situations or deviations in the application of current criteria.

Not all the entities’ processes have the same level of criticality with respect to compliance with the AEPD's objectives, so the different use cases have been classified according to the level of risk they present (see Appendix).

The detailed analysis of these threats and the impact they could have depending on the type of GenAI system that is implemented in the processes is developed in a document annexed to this general policy.

5. GenAI GOVERNANCE, POLICY AND MANAGEMENT

This section includes the set of structural measures implemented by the AEPD to achieve the objectives set with the implementation of GenAI systems. It is made up of:

- By a model of internal governance in relation to the GenAI.
- By the set of policies that determine the framework measures that will guide the implementation of the use cases and that will be adapted to the criticality of the processes and the impact that the materialization of a threat may entail.
- By the set of basic procedures to implement these policies, without prejudice to extending them according to the needs detected.

A) Internal governance

A governance model is established for the implementation in the AEPD processes of GenAI systems that handle personal or non-personal data[6]. Its purpose is to achieve all the objectives set by the AEPD (see section II).

The structure of AI governance includes the participation of all levels of the organization, to reconcile priorities, streamline conflict resolution, and involves external actors and fosters inter-institutional collaborations promoting good practices, common tools, and lessons learned.

The following roles are established in the AEPD:

- **Organisation Manager**, the authority that decides to use or develop one or more GenAI systems within the AEPD's use cases. In the case of the AEPD represented by the President.
- **Functional managers of the use cases**, in charge of defining objectives, requirements and monitoring effectiveness. In the case of the AEPD, the Deputy Director Generals, the Directors of the Division, the head of the Press and Communication Office and the head of the Legal Office.
- **Technical managers**, in charge of the implementation, maintenance and security of the systems. In the case of the AEPD, the General Secretariat.
- **Data Protection Officer**, who will ensure compliance with the GDPR and the application of proactive responsibility.

[6] The AEPD does not intend to establish interpretations on data processing that is not within its competence, but it is obliged, like any other organisation, to implement an information policy that complies with all the regulations and with its objectives of effectiveness and efficiency.

- **Information security officers**, in charge of guaranteeing the confidentiality, integrity and availability of the systems. In the case of the AEPD, the Deputy Director General for Promotion and Authorisations.
- **AI Manager**, who will coordinate strategic deployment, supervision, cross-cutting dialogue between units and monitoring of good practices. In the case of the AEPD, the Technological Innovation Division, represented by its Director.

B) POLICIES

This general policy, in the inclusion of GenAI systems in the use cases, will follow the following policies for their design, implementation, operation and maintenance:

GenAI SOLUTION TYPE SELECTION POLICY

GenAI systems could be part of the organisation's processes with varying degrees of integration:

- Inclusion or modification of a phase of the process by means of GenAI, without there being an integration into the organization's information systems, as may be the case of the text correction stage when it is used through a service accessible through a browser.
- Functions integrated into office tools or workflow tools that involve interaction with GenAI systems and possible connections with external tools when the user has full control of the information with which the GenAI interacts. For example, when a user has a particular document open and uses the GenAI on that document for translation, summarization, or others.
- Full integration into the corporate office environment, where the GenAI system is an inseparable element that intervenes in the entire administrative workflow including all types of tools in the environment and storage media, which implies possible access of the GenAI system to all the information processed in the organization's office environment and connectivity with external utilities through the Internet.
- Integration into the organization's ICT infrastructure, at the level of operating system and communications.

In turn, GenAI's systems allow for three basic approaches to implementation:

Approaches	Strengths	Weaknesses
Third-party GenAI systems deployed on infrastructure outside the organization's control, used as SaaS under	• Inefficiency of AI systems • Ease of use • High power • Interface via web or API • Less maintenance	• Disclosure of personal, end-user and citizen information, sensitive and confidential to third parties. • User profiling possible

their terms of use (External System): They are managed and maintained by third-party providers and are accessible through online platforms. In turn, they can be integrated into larger systems. They can be used to implement a phase in the procedure (access through browsers to services such as ChatGPT, Perplexity, Mistral, ALIA, etc.) or integrated into the office environment such as Microsoft 365 Copilot.	• Greater technological evolution	• Lack of control over data flows. • Lack of control over versions. • In the long term, lack of control of financial costs. • Difficult automation of employee usage policies for each GenAI system. • Possibility of hallucinations and irrelevant correlations. • No repeatability control • No control over biases. • Possible lack of traceability in data flows • No possibility of auditing • Exposure to attacks via the Internet: potential vulnerabilities in interfaces, APIs and others. • Unilateral changes in ToS and product discontinuity. • Very limited explainability.
GenAI systems developed by third parties and deployed in infrastructure under the control of the organisation (Internal System): The model is implemented on your own infrastructure or in a private cloud. Generally, although not limited to, using open weight models such as Llama, Qwen, Gemma or Mistral. Also**,** solutions under commercial license that can be deployed entirely on the organization's own infrastructure, including models.	• Inefficiency of AI systems • Auditable • Possibility of traceability of data flows. • Protection from the design of the flows personal, end users and citizens, sensitive and confidential information. • Control over the execution environment. • Integration with internal systems. • They allow for greater design of custom interfaces. • Financial cost control. • Allows for the development of controlled explainability tests	• They require a higher initial investment. • They require more training of personnel • They require more maintenance. • Possibility of hallucinations and irrelevant correlations. • Resource-dependent technological evolution. • Little control over biases.
GenAI systems developed internally or by third parties	In addition to the advantages of the previous one:	• They require a higher initial investment.

under custom specifications and deployed in infrastructure under the control of the organization and integrated with internal systems (Ad-hoc System): They offer the highest level of customization and control (see Appendix). They include open source models on which a fine-tuning process adapted to specific needs is carried out.	• Maximum level of suitability for specific use cases. • Better hallucination removal. • With specific knowledge integrated. • Control over biases. • Greater explainability.	• They require more maintenance. • They involve a post-development process with own resources and/or external hiring. • Resource-dependent technological evolution.

Each of these implementation approaches, in combination with the various levels of integration, has different advantages and disadvantages, poses different risks to meeting the objectives of this general policy, and allows for different effective implementation of the policies that follow are deployed.

As set out in the procedure for incorporating use cases, the most appropriate approach and level of integration for the incorporation of GenAI systems in each use case must be selected based on the risk assessment for compliance with the objectives of this general policy. The Annex shows the result of the analysis in a non-exhaustive way to determine the most appropriate solution for each process and use case.

POLICY ON THE PROCESSING OF PERSONAL AND SENSITIVE OR CONFIDENTIAL INFORMATION

Each use case will have a different degree of access to personal and sensitive or confidential information, and there are cases in which such access will be null and void. This circumstance should be carefully evaluated during the procedure to incorporate each use case. Such an assessment should analyse, in particular, whether measures have been put in place to prevent the processing of personal information of the GenAI system user himself.

- Use cases involving the processing by an GenAI system[7] of personal, sensitive or confidential information shall be implemented, in application of the precautionary principle:
  - Preferably in internal or *ad-hoc GenAI systems.*
  - In the event that the above approach prevents the achievement of other objectives of this general policy, they may be implemented in external GenAI systems that provide evidence of compliance with this general policy, beyond mere contractual representations or commitments.

[7] The use case may be implemented, for example, in a process that is a processing of personal data, but the GenAI is not used to process such data.

USE CASE DESIGN POLICY

- Use cases that require the processing of personally identifiable information and sensitive or confidential data with GenAI systems shall be implemented in GenAI systems that allow the organization to maintain operational control and direct oversight over confidentiality measures and purpose limitation assurances

- In the design and implementation of the GenAI use cases, the following will be analysed and verified:

  - That the tools used present simple interfaces and understandable work environments, adapted to the technical level of the user personnel, with visible instructions on the correct way to request, review and reuse the results generated.

  - There is clear and sufficient information or documentation on the general functioning of the model, including information on the type and approximate origin of the data used in its training, known limitations, and possible biases identified.

  - That the content generated (texts, images, summaries or reports) is reviewed and contrasted by competent personnel, using institutional or verified sources, and that the procedure establishes collaborative validation mechanisms when the results may have an impact on decisions or official documents.

- In the GenAI systems developed or managed directly by the AEPD, traceability mechanisms and basic recording of interactions must be incorporated, [8] which allow the identification of the uses made, the user profiles and the declared purpose, without unnecessarily preserving the content generated. These records will facilitate internal oversight and compliance with responsible use policies.

- In the case of external solutions or integrated into platforms not controlled by the AEPD, complementary organisational and technical control measures will be adopted, such as limiting access to previously authorised environments, expressly prohibiting the introduction of personal, confidential or unpublished information, and the incorporation of visible notices or reminders about the permitted use. A basic register of accesses and purposes may also be established in order to guarantee traceability and ensure safe use in accordance with internal rules.

- Any substantial changes in the scope of a use case, its impact, the natural persons affected, the performance of the model, etc., should be treated as a new use case.

[8] References to traceability and recording in this policy are used exclusively in the sense of internal control, organisational management and basic verification of the responsible use of the systems. They should not be understood as a reference to the traceability, registration or documentation requirements provided for in the Artificial Intelligence Regulation for high-risk systems, nor as an assessment or application of that regulatory framework.

AVAILABILITY AND RESILIENCY POLICY

- Development of continuity and backup plans, which in the event of failure or unavailability of the GenAI system ensure the operation of the process in which the use case has been implemented.

- Selection and implementation of GenAI systems in a way that does not create vendor lock-in.

- In those use cases in which the GenAI system plays a critical role for the continuity of processes that, in turn, are key to the organization, measures must be implemented to guarantee such continuity. For example, ensuring the possibility of having access to more than one GenAI system, that there is a real and effective possibility of migrating between GenAI systems and with interoperability between the information that is necessary for the execution of the processes.

- Control of the commissioning of new GenAI system releases:

    - In external GenAI systems, information on new versions, in particular control of opting for the new version, and information with evidence of tests of the system's behaviour or new limits and context of use, is guaranteed by contract.

- In case of internal systems development:

    - Isolation of training and execution environments to prevent the spread of failures or vulnerabilities.

    - Training in secure environments, with version control and pre-validation before moving to production.

    - Use of reversible fine-tuning techniques (such as LoRA or Adapters) that allow the upgrade or removal of specific components without affecting the entire system

- Monitoring of RAG systems through source validation, controlled deletion and protection against malicious injections in those use cases

TRANSPARENCY POLICY REGARDING THE USE OF GenAI

In relation to transparency:[9]

- The procedures, their execution and the decisions made within the framework of this general policy will be documented, guaranteeing their traceability and conservation.

[9] The reference to transparency in this policy is used exclusively in an internal organisational sense and is not related to the transparency obligations provided for in Article 13 of the Artificial Intelligence Regulation for high-risk systems, nor should it be understood as an interpretation or development of that regime.

- Mandatory inclusion of GenAI systems in the agency's digital asset inventory, classifying their criticality, purpose and relationships with other systems, accessible to all employees.

- In the selection or development processes of GenAI systems, the incorporation of access control, usage registration and traceability mechanisms will be required, especially in environments that can be connected with internal or sensitive documentation (for example, RAG systems or document platforms).

- A documented incident management process will be established in relation to GenAI.

- Interfaces and work environments should make the user visible when interacting with an GenAI system and include messages or reminders about the conditions of use and the need for human review of the results.

- The AEPD will continuously monitor the use of the GenAI through indicators of responsible use and quality of results, also verifying compliance with the contractual conditions, security guarantees and confidentiality agreed with the suppliers. This monitoring will be limited to internal use in the AEPD, not including the audit of the models or the data used in their training.

EXPLAINABILITY POLICY

In those GenAI systems used directly or indirectly for decision support, their selection in a use case will take into account:

- The information you provide about the sources used.

- Information you provide about how you dismiss certain sources or avoid certain answers.

- The information about the reasoning steps used.

- The user's ability to select or restrict fonts.

- If there is and information on the quality of the response is provided.

- Access to, or possibility to create, a "Golden data set" or high-quality dataset for use as a reference to evaluate and validate the operation of the system.

- If the vendor provides results of the evaluation performed on performance metrics that may be appropriate for the specific use case.

POLICY REGARDING AUTOMATED DECISIONS AND THEIR MONITORING

The following policies shall be followed in the design of the implementation of an GenAI system in a process:

- In the implementation of GenAI systems in the AEPD's processes, there will be no automated decisions based solely on automated processing, including profiling, that produces legal effects on the AEPD or significantly affects it in a similar way.

- In the implementation of GenAI systems in AEPD processes, the precautionary principle will be applied so that there is no margin of doubt in the application of the previous paragraph.

- All decision support systems used in AEPD processes when they affect fundamental rights, procedural guarantees, have legal effects or may jeopardize the objectives of this policy, will be implemented with the following safeguards:

    - The process in which the GenAI system is included must contemplate prior human validation and control, in any case[10].

    - Training will be carried out for users (see human resources policy and continuous training procedure for personnel) to effectively comply with human supervision.

    - A workload assessment shall be included in the monitoring procedure to determine whether effective human intervention is possible.

    - The recommendations of the Technical Note on Human Supervision of the European Data Protection Supervisor shall apply[11].

POLICIES REGARDING THE PROTECTION OF FUNDAMENTAL RIGHTS AND PROCESSING OF PERSONAL DATA

The assessment and management of risks to fundamental rights shall be governed by the applicable legislation in each case, including, where applicable, the instruments provided for in the GDPR and in national public sector law. If, at a later stage, a system falls within the scope of Article 6(2) of Regulation 2024/1689, on artificial intelligence, it would be appropriate to carry out the impact assessment required by that Regulation, in which case the specific guides, procedures or instruments provided for in that regulatory framework should be used.

Likewise, a Data Protection Impact Assessment may be carried out when:

- the use case involves a processing of personal data that entails a high risk to the rights and freedoms of natural persons (in this case there will already be a DPIA that will have to be reviewed when part of the nature of the processing changes).

- the use case involves the processing of personal data to which one or more high-risk systems are incorporated according to Regulation 2024/1689 (RIA).

[10] The references to human supervision in this policy are used in the proper sense of risk management, organisational control and, where appropriate, the provisions of the GDPR for automated decisions. They should not be interpreted as a reference to the human supervision requirements set out in the Artificial Intelligence Regulation for high-risk systems or as an analysis under that Regulation.

[11] EDPS TechDispatch #2/2025 - Human Oversight of Automated Decision-Making

Beyond compliance with data protection regulations, the following measures will be taken in the design and implementation of an GenAI system within a process:

- In terms of the exploitation of the GenAI systems in each use case:
  - The ability of GenAI systems to access the organisation's data, and data relating to users, will be configured by applying the principle of minimisation and limited data retention, both metadata and user memory, according to the needs of the use case.
  - Procedures will be designed, or tools will be implemented to prevent the accidental inclusion of personal or confidential data in the prompts or files that the GenAI system can access.
  - In RAG-type GenAI systems that require access from external servers to the organization's data, anonymization or pseudonymization techniques must be implemented in the sources used, reducing the exposure of identifiable information.
- Regarding the design of ad-hoc GenAI systems[12]:
  - Application of measures that prevent uncontrolled enrichment of datasets (training and retrieval), respecting the principles of purpose limitation and minimisation.
  - Application of anonymization and pseudonymization techniques before training and in the sources used by RAG systems that involve communication to external GenAI systems.
  - Consideration of the use of Differential Privacy techniques in the data used for evolution or fine-tuning, to reduce the possibility of memorization of personal data in the model.
  - Documented verification that the form does not incorporate personal data or, where applicable, that access is strictly limited to the need-to-know principle.
- Establishment of technical and organisational mechanisms to protect the rights and freedoms of data subjects, both in the processing and exposure of structured, anonymised data or internal documents.

CYBERSECURITY POLICY

In the implementation of the GenAI system in the processes, it must be ensured:

- GenAI systems shall be subject to ENS categorisation and shall comply with the principles and measures corresponding to the resulting level. Where the use case involves sensitive information, high-level personal data or critical functions, 'high-level' controls will be adopted.

[12] Open-source models refined through fine-tuning processes

- In addition, recognised good cybersecurity practices will be followed, both in the public sector and in the general technological field[13], which are specific to the use of GenAI systems and according to the risk to achieving the objectives of this general policy. In particular, in compliance with Article 32 of the GDPR.

- The AI Manager will monitor new threats and vulnerabilities in the state of the art and context of GenAI solutions and the Technical Manager in the specific GenAI systems deployed in the organization. The implementation of GenAI systems in use cases will have to be reviewed in the face of the severity of the new threats and vulnerabilities detected.

- Application of the AEPD's Information and Security Policy.

- The use of GenAI's systems will be in accordance with the AEPD's corporate access control and activity logging policies. For each use case, the corresponding digital identity scheme will be evaluated and documented, determining which profile is accessed – for example, personal identification of the employee, generic accounts of a unit, technical or service identities, temporary access linked to projects or other authorized modalities that are appropriate for the use case or for the operational needs of the organization. The option selected must be consistent with the assigned functions and the specific needs of the use case.

- Inclusion of the particularities of GenAI systems in the incident management process in relation to, for example, identification of biases, performance or availability issues.

- Isolation of critical environments. Systems that operate with classified or high-impact information for the fulfilment of the objectives of this general policy must be logically or physically isolated from other networks, especially the internet.

HIRING POLICY

When contracting GenAI solutions, especially when it comes to external or cloud services, at least the following aspects must be evaluated in advance and documented:

- The processing of metadata/cookies: what technical and usage data is collected (logs, identifiers, telemetry, device signature, etc.).

- Explicit statements of whether the provider declares, does not declare, or at what level it uses the content of conversations/files to improve services/models and under what conditions.

- Existence and extent of mechanisms to exclude user content from training (account controls).

[13] If the AI solution that is implemented is Microsoft-Azure, in addition, the ICT SECURITY GUIDE CCN-STIC 884D will be followed.

- Possibility of configuring by the administrator the cancellation of requests for opinions or the degree of satisfaction to end users (feedback).

- Possibility of configuration and control by the administrator of manual reviews carried out by the conversation or file provider and under what guarantees.

- The location of data: where it can be stored/processed (US/EU/other regions)

- GDPR compliance.

- Data retention time: Timeframes or criteria for retaining chats and user content.

- The control and information provided about the deployment of new versions and their characteristics.

- The stability of the contract and terms of service. Evaluation of the stability and predictability of the terms of service, including continuity, confidentiality and security clauses.

- If, at a later stage, it is found that the solution to be contracted could fall within the scope of application of the RIA, the legal regime established by said Regulation shall apply.

HUMAN RESOURCES POLICY IN RELATION TO THE GenAI

- It will be an essential requirement that any user of these technologies receives specific and continuous basic training on their correct use, their limitations, good practices and associated risks, taking into account, among others, the context of the use cases and the people or groups of people foreseeably affected.

- The AEPD's annual training plan, and after consulting the IA Manager, will include the execution of three types of continuous training of personnel with the following aspects:

  - About this general policy.

  - On each of the GenAI systems that are necessary to perform its functions. In particular, on prompt engineering, interpretation of outputs, identification of biases and errors, and incident management, among others.

  - Technical training for ICT teams in the design, maintenance and control of automated and intelligent systems on artificial intelligence systems and to identify opportunities and risks.

- User-guides and training materials for employees, including this general policy, will be available online.

- A channel is established for two-way communication with employees by Human Resources, beyond incident management, to report changes in functionality or new risks, avoid uncertainty or misunderstandings among staff, as well as to collect their suggestions on new opportunities and possible use cases.

- The monitoring plan shall include an analysis of whether the introduction of GenAI is accompanied by an overload of work, unplanned task replacement or loss of functions without relocation.

EMPLOYEE USAGE POLICY

- The use of GenAI systems for the execution of the work follows the same restrictions that apply to any system or personal device in relation to the AEPD Security Policy.
- The use of the GenAI system shall be restricted to users who have received appropriate training, in particular on these policies.
- Do not use an GenAI system that has not been registered in the GenAI system inventory.
- GenAI systems must be used only for the purposes set out in each use case, and within the limits of the capabilities indicated in the documentation.
- In the internal distribution of material generated with GenAI, the use of GenAI and the extent to which the content is fully generated by GenAI will be communicated.
- All content generated by GenAI will be reviewed by the user. If it is aimed at a hierarchical superior or intended for publication, it will have to pass an internal peer review.
- All content generated by GenAI intended for institutional communication will undergo a regulatory compliance review, in particular intellectual or industrial property, by the Press Office.
- The results generated by GenAI systems must be compared with reliable sources, internal documentation or collaborative validation, especially when they affect critical processes or decisions relevant to citizens or entities.
- The use of sensitive non-personal information, such as institutional references, names linked to serious incidents or internal documents, even if they do not contain personal data, that may damage the corporate image or the institutional strategy of oneself or third parties, will be minimised to what is strictly necessary.
- In the use of GenAI systems, the AEPD's corporate access control and activity logging policies will be applied, adjusting their configuration to the corresponding use case and the provisions of the Security Policy section.
- Use cases of special sensitivity or complexity may require specific policies or terms of use that extend what is established in this document, which must be respected by users.

OVERSIGHT POLICY FOR THIS POLICY

- A procedure for monitoring compliance with this general policy is established.

- Regular monitoring of all use cases is established.
- An GenAI incident management procedure is established integrated into the AEPD's incident management system.

C) PROCEDURES

PROCEDURE FOR DRAFTING, APPROVING AND REVISING THIS GENERAL POLICY

- This general policy will be prepared and maintained by the IA Manager following the guidelines of the Organisation Manager.
- The functional, technical and information security managers will be subject to prior review by the DPO.
- They shall be submitted to the Head of the Organization for approval.
- The IA Manager will initiate a policy review cycle when:
    - It is established by the Head of the Organization.
    - Incidents occur that compromise compliance with the objectives of these policies.
    - New use cases are identified.

HOW TO INCORPORATE A USE CASE

The procedures described below will be applied with a proportional and flexible approach, depending on the nature and complexity of the use case. Simplified templates or mechanisms may be used, and common documentation may be developed for several use cases with similar characteristics, provided that the traceability of decisions, the identification of those responsible and consistency with this general policy are ensured.

- Identification of needs by the Functional Manager within the framework of the AEPD processes.
- First evaluation and, where appropriate, design by the AI Manager, which will include:
    - A risk analysis in relation to the threats identified in this policy and those of the process in which the use case is included.
    - Carrying out the appropriate Proofs of Concept.
    - A recommendation on whether to include GenAI, and if applicable, the type of environment to choose.

  - A design of the use case process that contemplates the implementation of the aforementioned policies.

- Review of the assessment by the DPO (if applicable), Technical Manager, Security Manager and Legal Office (if applicable) to determine regulatory compliance (both data protection and any other applicable regulations).

- The Functional Manager will prepare a document with the design requirements of the use case that will be submitted to the Head of the Organization, which includes, among others:

  - Regulatory compliance documentation (both data protection and any other applicable regulations).
  - Implementation of the general policy.
  - Identification of the needs for transparency, explainability, measures in relation to automated decisions, training and supervision.
  - Validation and version control criteria.

- Approval by the Head of the Organization.

PROCEDURE FOR DESIGNING AND DEPLOYING A USE CASE

- The Technical Manager will prepare, based on the design requirements:

  - Preparation of a design plan for the use case.
  - Preparation of a deployment, maintenance and removal/replacement plan.
  - Preparation of a verification and validation plan.
  - Preparation of a contingency plan.
  - Preparation of guides, materials, policies and specific training plan (if applicable).

- The Technical Manager will submit it to the approval of the Head of the Organization, who will carry out the consultations he deems appropriate to verify compliance with said general policy.

- Once approved, the Technical Manager will carry out the implementation and deployment of the system.

- The Technical Manager will carry out and document the verification and validation plan, the results of which will be verified with the AI Manager and, if satisfactory, will submit to the Head of the Organization the decision to put the system into operation.

- The Technical Manager shall record the GenAI system in the inventory.

INCIDENT MANAGEMENT PROCEDURE

- Any incident will be reported with a support ticket to the Technical Manager.
- The communication of the incident must state:
  - Inefficiency of AI systems
  - Infrastructure insecurity and lack of process continuity
  - Wrong, irresponsible, or harmful human interaction with AI
  - Bias and discrimination
  - Impacts on rights and freedoms in relation to data protection.
  - Disclosure of Non-Personal Information
  - Lack of governance and loss of institutional integrity
  - Lack of transparency and explainability of actions based on GenAI
  - Impact on employee rights
  - Lack of coherence in similar situations or deviations in the application of current criteria.
- The Technical Manager will report the incident to the AI Manager, who will classify it as minor or serious.
  - In the event of minor incidents, the AI Manager will issue the appropriate recommendations to the Controllers that it deems appropriate.
  - In the event of major incidents, the AI Manager will:
    - It will immediately notify the Head of the Organization and, where appropriate, the DPO.
    - He will propose to the Head of the Organization the actions that are necessary.
    - The Head of the Organization, in the event that the incident affects a high-risk system according to the RIA, will execute the obligations imposed by article 73 of the RIA.
    - It will initiate a monitoring process.

PROCEDURES FOR MONITORING THIS POLICY

- The supervision process will be initiated by decision of the Head of the Organization, and by indication or consultation with the other managers.
- The monitoring process will be suggested by the AI Officer:
  - Annually
  - Existence of a serious incident.
  - Monitoring of new threats and vulnerabilities in the state of the art and the context of GenAI solutions[14].
  - Alert from automatic monitoring tools.
- The monitoring procedure will follow a risk-based approach, prioritizing use cases with the greatest impact or where a major incident has occurred.
- The monitoring procedure will be carried out through an internal or external audit depending on the urgency and availability of resources.
- The supervisory actions shall verify the application of this general policy, in particular:
  - Identification of incidents and possible solution.
  - Compliance Review
  - Compliance with the principles established in the policies, in particular in relation to human supervision and permitted uses.
  - Problems identified in the achievement of the AEPD objectives through the established metrics and possible solution.
  - Evaluation of the Return on Investment (ROI)[15], in particular unexpected cost overruns, internal financial impact due to maintenance, licenses or poorly sized scalability.
  - Periodic vulnerability assessment. Depending on the criticality of the system, checks will be carried out on the robustness of the GenAI system against state-of-the-art threats (e.g. prompting attacks).

[14] Known attacks on other organizations, publicized vulnerabilities, regulatory changes of services dependent on other countries, contractual changes, changes in relevant political, economic, or social contexts.

[15] Understood before in monetary terms, in terms of improving the service to citizens.

- The outcome of the monitoring process shall be documented, including, if applicable, recommendations on the adaptation of the GenAI system or the procedures of the process in which the use case is implemented, its replacement or removal from the GenAI system.

- It will be submitted to the decision of the Head of the Organization.

6. CONCLUSIONS

This document establishes a general policy for the implementation, governance and responsible use of generative artificial intelligence systems within the AEPD. Its purpose is to strengthen the Agency's technological and organisational capacity, ensuring a digital transformation that is safe, ethical and fully compliant with the current regulatory framework. As noted, this policy is not an instrument for compliance with or development of the Artificial Intelligence Regulation. Likewise, and as has been explained, it does not incorporate in any case the classification of systems in accordance with said Regulation, including high-risk cases. Overall, this policy seeks to position the AEPD as a pioneering institution in the responsible, legal and transparent use of artificial intelligence and automation in the Public Administration. The progressive implementation of the systems, under solid governance and with human supervision, will allow the Agency to improve its efficiency and technical capacity without renouncing its founding principles: the defence of rights, the protection of privacy and institutional exemplarity.

This document therefore provides a realistic, balanced and rigorous roadmap to address technological transformation in a safe, controlled and aligned way with the public interest. Its implementation must be accompanied by a continuous process of evaluation, adaptation and improvement, which allows responding to technological advances, regulatory changes and social expectations, thus consolidating a mature, ethical and sustainable institutional intelligence.

7. REFERENCES

- Spanish Data Protection Agency (2020) GDPR compliance of processing that embed Artificial Intelligence. An introduction

- Spanish Data Protection Agency (2020) Data Governance and Data Protection Policy

- Spanish Data Protection Agency (2021) Risk Management and Impact Assessment in the Processing of Personal Data

- Spanish Data Protection Agency (2021) Audit Requirements for Personal Data Processing Activities involving AI

- Spanish Data Protection Agency (2023) Approach to data spaces from GDPR perspective

- Spanish Data Protection Agency and European Data Protection Supervisor (2022) 10 Misunderstandings about Machine Learning

- Spanish Association for the Study, Promotion and Development of the Framework of Professional Competences in Public Procurement (2024) Practical Guide for the Use of Generative AI by Public Employees

- Comisión Europea (2019) Ethics guidelines for trustworthy AI

- Comisión Europea (2024) A strategic vision to foster the development and use of lawful, safe and trustworthy Artificial Intelligence systems in the European Commission

- Comisión Europea (2024) Guidelines for staff on the use of online available generative artificial intelligence tools

- Comité Europeo de Protección de Datos (2024) Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models

- Commission Nationale de l'Informatique et des Libertés (2025) AI and GDPR: the CNIL publishes new recommendations to support responsible innovation

- Commission Nationale de l'Informatique et des Libertés (2025) AI: Guaranteeing the security of the development of an AI system

- European Medicines Agency (2024) Harnessing AI in medicines regulation: use of large language models (LLMs)

- Information Commissioner Office of UK () AI and data protection risk toolkit

- Information Commissioner Office of UK (2025) Internal AI Use Policy

- Office of the Privacy Commissioner for Personal Data of Hong-Kong (2025) Guidelines for the use of generative AI by employees

- Organisation for Economic Co-operation and Development () Recommendation on artificial intelligence

- Organization for Economic Cooperation and Development and United Nations Educational, Scientific and Cultural Organization (2024) G7 toolkit for artificial intelligencein the public sector

- Prof. Dr. Johan Wolswinkel - Council of Europe (2022) Artificial intelligence and administrative law

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)

- European Data Protection Supervisor (2023) TechSonar - Large language models (LLM)