January 2026

SUMMARY OF OBLIGATIONS AND RECOMMENDATIONS

FOR THE MANAGEMENT OF GENAI IN THE AEPD

Within the framework of the "General Policy for the Use of Generative AI in Administrative Processes of the AEPD" published in November 2025 and the annex that establishes a practical framework for the safe, ethical and controlled application of AI in the AEPD, in December 2025, the main obligations and recommendations addressed to the decision-making bodies and teams in charge of implementing use cases of Generative AI (GenAI) in the organization's workflows and processing activities:

Governance

- Accurately identify the decision-making and execution roles in accordance with GenAI's internal usage policy, especially the functional managers and technical managers for the management and supervision of the operation of the GENAI system for each use case.
- Ensure prior approval of each use case before its implementation following the new use case design and deployment procedure.
- Maintain an up-to-date record of the GenAI systems in use in the digital asset inventory, documenting how they operate, purpose and level of risk.
- Define and implement a procedure for managing the life cycle of GenAI systems from proposal to retirement, which applies measures to ensure regulatory compliance commensurate with the risks of the processes and treatments in which it is included.

Design and development of use cases

- Consider the use of GenAI as a support for human function, not as a substitute for it.
- Ensure understandable and secure interfaces, adapted to the technical level of the end users.
- Document the general functioning of the models used, their sources, limitations and known biases.
- Implement systematic mechanisms to detect and correct errors.
- Regularly evaluate the performance of the system, ensuring its compliance with ethical and legal principles.

Processing of personal data and information, sensitive or confidential

- Apply the principles and obligations established in data protection regulations in those cases of use that involve the processing of personal data: minimisation, limitation of purpose and proportionality in the use of personal data, facilitate the execution of rights and, where appropriate, update the Data Protection Impact Assessments (DPIAs) of the processing when the GenAI systems undergo significant modifications.

- Implement use cases that deal with personal, sensitive or confidential information, preferably in internal systems or in ad-hoc systems that guarantee the control of the organization.
- Establish the necessary mechanisms to prevent users from entering personal, sensitive or confidential information into systems that are not explicitly authorized to process such data.
- Configure AI systems by applying the principles of minimization and limited data retention in terms of access to organizational data, user data, metadata, and system memory capacity.
- Implement effective validation and human control mechanisms in use cases that may involve automated decision-making based solely on automated processing that produces legal effects or significantly affects the rights and freedoms of individuals.
- Train users in effective techniques to formulate their prompts to the GenAI in a clear and effective manner, avoiding specific or irrelevant details that may compromise the privacy and confidentiality of personal information or data.

Transparency and explainability

- Ensure the explainability and transparency of automated decisions, if any, ensuring that they are understandable to citizens and allow for accountability.
- Ensure that GenAI systems are transparent about the sources used and the selection or discard criteria.
- Document the procedures and decisions related to the use of GenAI in each use case.
- Implement traceability mechanisms and activity records to verify the logic and context of each decision based on GenAI.
- Make visible in corporate application interfaces in which situations you are interacting with an AI and include mandatory human review notices.

Security and availability

- Subject GenAI systems to categorization in accordance with relevant national cybersecurity regulations and standards, and apply controls according to the resulting level.
- Implement encryption in transit and at rest, authentication, and role-based access control.
- Ensure the isolation of critical environments (systems that operate with classified or high-impact information) from other networks, especially the Internet.
- Establish security incident monitoring and response mechanisms that include continuous monitoring and incident management.
- Develop continuity and backup plans that ensure the availability of key processes, in particular, avoid lock-in to a single vendor.
- Align the use of GenAI systems with corporate access control policies.

- Avoid relying on GenAI for critical or urgent decisions: These tools should not be relied upon for processes that require maximum accuracy, immediacy, or security, as they can be unstable or unreliable

Contracting

- Before contracting GenAI systems, evaluate the processing of metadata, logs and telemetry, the use of data for training, to improve services or any other purpose by the provider.
- Also evaluate data location, retention periods, version control, and contract stability.
- In general, whenever external systems are chosen, guarantee the contracting of services in business mode that guarantees governance by the organization.
- Include data non-reuse and GDPR, RIA, and ENS compliance clauses in supplier contracts.
- Verify the existence of configurable mechanisms in relation to privacy settings, which allow disabling all those functionalities that may pose a threat to the privacy and security objectives pursued by the organization.

Human resources and training

- Restrict the use of GenAI systems to trained and authorised users.
- Assess the labour impact of the GenAI on the supervisory plan (overload or redistribution of duties).
- Ensure continuous training, regularly training users.
- Establish two-way communication channels, in relation to the use of GenAI in the organization's processes, between users and management teams, beyond incident management.

Responsible use of generative AI tools

- Develop specific limitations of use for GenAI systems that require it and train users on those limitations.
- Train users in the proper techniques to critically analyze any AI-generated response, allowing them to detect errors or biases. Warn them not to assume that the information is correct without checking it.
- Explicitly inform users of:
  - The prohibition of using GenAI systems not registered in the corporate inventory.
  - The obligation to manually review and validate the results generated before their use or publication.
  - The obligation not to share confidential information, never enter private data, non-public information or personal data.
  - The obligation to respect intellectual and industrial property.
  - The prohibition of including content generated by GenAI in texts that produce legal effects, in resolutions or in any official document without human review and validation.