aepd agencia española protección datos

2025-2030 Strategic Plan of the Spanish Data Protection Agency

Responsible innovation and defence of dignity in the digital era

Contents

1. INTRODUCTION, MISSION AND VISION 3

2. GUIDING PRINCIPLES 5

I. Independence 5

II. Innovation and adaptability 5

III. Internationalisation and influence 5

IV. Cooperation 5

V. Proactivity and prevention 5

VI. Excellence and technical quality 6

VII. Defence of the general interest 6

VIII. Open agency 6

3. AREAS OF ACTION 6

Area 1. An intelligent agency 6

Area 2. For technological innovation with guarantees 7

Area 3. Promote and support regulatory compliance 9

Area 4. Promote partnerships and collaboration with organisations and professionals 10

Area 5. Leadership and international and national strategic influence 11

Area 6. Effective and continuously improving administration 12

Area 7. Openness, proximity and a culture of data protection 13

Continuous evaluation and dynamic review of the Plan 14

1. INTRODUCTION, MISSION AND VISION

The objective of the 2025-2030 Strategic Plan of the Spanish Data Protection Agency, an independent administrative authority with powers in the protection of fundamental rights of individuals in relation to the processing of their personal data (hereinafter, AEPD or the Agency) is to have a strategy in the context of continuous digital transformation that governs its actions in a structured and orderly manner, enabling this Plan to achieve the proposed objectives.[1]

This Plan consists of a series of objectives which, in the form of guiding principles, will steer the Agency's course over the coming years.
To achieve these objectives, several lines of action are proposed, which will in turn consist of specific, measurable and achievable measures

Our **mission** is to effectively and proactively guarantee the fundamental right to personal data protection for citizens, with special attention to vulnerable groups. To this end, we are committed to privacy by design and by default as a priority approach.

Although essential, reactive mechanisms, such as the necessary power to sanction and correct, often intervene too late to fully repair the damage. Therefore, our strategic commitment is to actively promote prevention and cooperation with all the actors involved, with the shared goal of achieving the highest possible level of privacy and personal data protection. To this end, we will continue to publish guides, develop tools and offer practical and preventive guidance with the aim of promoting a culture of voluntary compliance.

In a context of constant change and technological uncertainty, the Agency will maintain a flexible and adaptable internal organisation and training structure, ensuring the necessary agility to respond to rapid and disruptive transformations resulting from digital advances and the adoption of new regulations. Internal systems for the continuous monitoring and anticipation of emerging technological trends will be strengthened, intensifying collaboration with research centres, universities and specialised professionals, in order to promote innovation in line with regulatory compliance.

Technological innovation and the constant emergence of disruptive technologies, such as artificial intelligence (AI), are an unstoppable phenomenon. Innovation can even be considered a principle or right insofar as it is aimed at improving human well-being, contributing to the effectiveness of fundamental rights and strengthening democratic values. However, advances also entail risks and potential negative impacts on privacy and data protection, which particularly affect those with special

[1] Article 9 of the Statute of the Spanish Data Protection Agency (AEPD, by its initials in Spanish) approved by Royal Decree 389/2021, of 1 June, states that the Presidency of the Spanish Data Protection Agency shall approve, in the first half of its term of office, a five-year Strategic Plan with the aim of laying the foundations for the Agency's lines of action during that period, incorporating specific actions.

protection needs. Data protection regulations must be interpreted in accordance with this principle of responsible innovation.

In this context, our **vision** is to consolidate the Spanish Data Protection Agency as a leading, proactive and internationally recognised authority that, focused on privacy and personal data protection, guides and channels these technological developments appropriately. The Agency will act with human dignity as its essential reference point, remembering that behind every piece of data there is a specific person whose rights and freedoms must be protected. This principle is the ultimate foundation and guide for all our work, even though it may sometimes be obscured by the high technical and regulatory complexity of data protection. The processing of personal data is the main channel through which significant impacts on privacy and the rights of individuals and groups are generated.

The AEPD's work is complemented by that of other public authorities with powers in areas such as consumer rights, financial services, telecommunications, the digital market and platforms. In these cases, we will collaborate within our respective areas of competence and work to continue actively influencing the European Union and other international forums on privacy matters, so that the Spanish and European vision has an impact on the global protection of personal data.

2. GUIDING PRINCIPLES

Based on the new technological, social and geopolitical realities, several principles have been identified that are considered appropriate for governing the activity of this entity over the coming years.

I. Independence

- The Agency is an independent body that must continue to ensure that its actions are governed at all times by full organisational, functional and decision-making autonomy, and must remain free from external influences or any political or economic pressure.

II. Innovation and adaptability

- The Agency will strengthen its agility and ability to adapt to technological and social changes, promoting a proactive culture of innovation that integrates data protection by design and by default.

III. Internationalisation and influence

- The Agency will work to improve its international standing and its capacity to influence decision-making in the international organisations of which it is a member.

IV. Cooperation

- The Agency will work to generate new partnerships and strengthen existing ones, both nationally and internationally, promoting cross-institutional collaboration and the joint creation of innovative solutions to improve the protection of citizens' personal data.

V. Proactivity and prevention

- The Agency's actions will be characterised by its anticipation of risks and challenges in the field of data protection, and will be carried out with a preventive approach based on awareness-raising, advice and supervision, with a view to preventing problems before they arise.

VI. Excellence and technical quality

- The Agency will maintain its commitment to technical rigour in all its actions, for which it will promote the continuous training of its staff and the improvement of its processes in order to reinforce the credibility, effectiveness and technical authority of the entity.

VII. Defence of the general interest

- The Agency's actions are aimed at effectively safeguarding fundamental rights and public freedoms related to privacy and personal data processing, promoting public trust and social equity in the digital environment.

VIII. Open agency

- The Agency's actions will be characterised by openness, transparency, accountability, and participation and interaction with citizens, privacy professionals, regulated sectors, and civil society.

3. AREAS OF ACTION

The Agency's objectives are organised around seven areas of action:

Area 1. An intelligent agency

The Agency aims to achieve smarter, more proactive and effective supervision, supported by technology and efficient, results-oriented management. Priority will be given to action where the greatest impact on the dignity and rights protected by data protection is identified, strengthening the capacity for rapid and proportionate response to possible infringements. Among the lines that make up this area, the following can be highlighted:

1.1. Adopt an “AI first” policy, always with guarantees, in all AEPD functions, applying emerging technologies to improve internal processes, research, document analysis and access to information and documentation, both internally and externally. Its implementation should serve as a benchmark for promoting responsible practices in the use of AI in the public sector. Intelligent complaint handling systems that support and streamline case resolution will be incorporated, as deemed appropriate.

1.2. Develop advanced monitoring systems based on AI and automated data analysis, enabling early risk detection, the definition of indicators, the use of compliance simulators and, where appropriate, the deployment of preventive audits and classification models based on historical trends.

1.3. Conduct proactive analysis of emerging sectors and technologies, prioritising those of a strategic nature due to their high impact on dignity, rights and freedoms and vulnerable groups. These sectors include healthcare, digital platforms and marketing aimed at minors, digital education, biometric and neurotechnological systems, work environments and digitised public administrations. The aim is to anticipate risks before they become widespread, issue early recommendations and, where appropriate, activate specific supervision and audit mechanisms, with the participation of civil society. At the same time, the admissions system will be evaluated and an internal system for the strategic prioritisation of cases will be implemented to detect and analyse those with particularly relevant legal or social implications, coordinating responses between the areas involved.

1.4. These strategic analyses will be complemented, to the extent of the AEPD's actual capabilities, with supervised testing environments that allow organisations to test new technologies or services with impact on privacy, using sector-specific compliance simulators designed by the AEPD, in order to anticipate risks and strengthen regulatory compliance before their widespread deployment.

1.5. Improve the efficiency and consistency of case handling through the strategic use of the accumulation of related procedures and the development of indicators to assess the impact and effectiveness of actions, particularly in the areas of supervision and sanctions.

1.6. Assess and encourage the development of tools for the automated analysis of privacy policies, cookie settings, public source code repositories and open databases on security breaches, in order to detect patterns of non-compliance and systemic risks.

Area 2. For technological innovation with guarantees

The Agency is clearly committed to responsible innovation with guarantees. Priority will be given to the supervision of emerging technologies such as AI, biometric systems and neurotechnologies, especially when they affect vulnerable groups. Through the Privacy Lab and in collaboration with experts, research centres and universities, a knowledge hub will be created and tools, guidelines and expertise will be developed. The AEPD will also strengthen its role in the coordinated implementation of new European regulations, ensuring effective governance that respects fundamental rights and freedoms. The following lines of action are particularly noteworthy in this area:

2.1. The Agency's work will focus on the risks to data protection posed by AI, including generative systems, autonomous agents and recommendation algorithms, as well as biometric and facial recognition systems, data spaces, neurodata, quantum technologies, blockchain and digital platforms, with a particular focus on vulnerable groups such as children, older people and others in need of special protection.

2.2. The Privacy Lab, in close collaboration with leading centres and universities, specialists and professionals, will observe, analyse and collaboratively research emerging technologies such as AI, quantum and neurotechnologies and the new challenges and impacts they pose for data protection. This space will promote the generation and exchange of knowledge, guidelines, tools and best practices, prioritising, where possible, the development of free, transparent and open-source solutions. An editorial line will also be developed, including an academic journal as well as agile, dynamic and interactive external content of interest, by and for the community of privacy specialists and professionals.

2.3. The development of specialised technical guidelines will be promoted to strengthen governance in the digital economy and provide guidance on the responsible application of technologies. These guidelines will include criteria on appropriate legal bases for the processing of personal data and establish standards for transparency and human oversight in automated decisions. Existing materials on risk analysis and impact assessments will also be updated to incorporate new challenges related to the use of AI.

2.4. The role of the AEPD is essential in the new EU digital regulations (data, data governance, health, platforms and political advertising). To this end, the role of the Agency in each case will be studied, along with the best ways to effectively carry out its role in collaboration with sectoral authorities, the public sector and European regulatory bodies.

2.5. In the context of the Artificial Intelligence Regulation, the technical and organisational capacity of the AEPD will be designed and strengthened for the supervision of AI systems, in particular those that are prohibited and high-risk and legally assigned, through the development of internal instruments (assessment protocols, alert channels, incident management) and its own technical capabilities (laboratories, databases, analysis models) that enable a swift and informed response to serious risks or breaches. In this context, active participation will be ensured in the network of national and international competent authorities, as well as in the context of the Council of Europe's AI Convention.

2.6. The AEPD will encourage the creation of public registers and inventories of AI data processing in the public sector. These are a mechanism for improving algorithmic transparency, guaranteeing data protection principles and rights, and facilitating the supervisory work of data protection authorities.

Area 3. Promote and support regulatory compliance

The Agency aims to facilitate compliance with data protection regulations by all actors, especially micro-SMEs, start-ups and SMEs, self-employed persons and public administrations, by promoting a culture of responsible compliance that is simple and adapted to each context. The Agency's guidance role will be strengthened through guides, practical tools and specialised support channels with AI support. Data Protection Officers (DPOs) will be given a central role as key figures in this support and, where appropriate, sectoral self-regulation mechanisms such as codes of conduct will be promoted. Initiatives to simplify regulations and improve interoperability between regulatory frameworks will also be promoted in Spain and at European and international level. Within this area, a number of lines of action are particularly suitable for achieving the objective set:

3.1. The Agency will strengthen its guidance role by developing and continuously updating specific guidelines tailored to the needs of different sectors and groups. These guidelines will address key issues such as informed consent for minors, age-appropriate design, data protection techniques from the design stage, data deletion and blocking, digital identity, roles in automated processing and guarantees of human oversight in automated decisions. In addition, it will promote the systematic inclusion of an “SME clause” with simplified guidelines, and relevant documents from authorities such as the European Data Protection Supervisor (EDPS), the CNIL, the ICO and those produced within the framework of the European Data Protection Board (EDPB) will be disseminated. The publication of sectoral guidelines based on good practices, real examples and frequently asked questions will also be promoted.

3.2. Specific resources, technical kits, self-assessment tools and differentiated service channels will be developed, including digital services aimed at minors.

3.3. Interoperability between risk analysis and management methodologies —such as ISO 27005 or the National Security Scheme— will be promoted, encouraging their alignment with the data protection approach. This perspective will also be integrated into sectoral regulatory frameworks such as DORA, NIS2 and PSD2, in order to strengthen consistency between cybersecurity obligations and guarantees for individuals' rights and freedoms.

3.4. The website will be enhanced with a clearer sectoral structure and an advanced search system based, where possible, on AI, allowing more efficient access to decisions, reports and consultations. Virtual assistants will also be strengthened to respond quickly to basic queries, and a specialised consultation channel will be set up for highly complex sectors, promoting legal certainty.

3.5. A system of self-assessment of compliance with the General Data Protection Regulation (GDPR) and the Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD, by its initials in Spanish) in the public sector will be promoted through partnerships with regional authorities, provincial councils and municipalities, with a view to diagnosing the compliance situation, encouraging improvement and enabling the AEPD to identify areas of concern that will guide institutional support policies.

3.6. The possibility of channelling actions, complaints and claims through a preliminary channel before the DPO, where one exists, before formally initiating the AEPD's action will be assessed.

3.7. The guarantees for the exercise by the data subject of the right to object and not to receive unwanted commercial communications will be strengthened.

Area 4. Promote partnerships and collaboration with organisations and professionals

Privacy and data protection require a joint effort involving professionals and various entities. The Agency will strengthen its role as an active institution through a structured map of strategic alliances with public, private, academic and third sector authorities and entities that are key to ensuring privacy in areas such as health, education, justice, children and AI. This cooperation will be coordinated using a cross-cutting management and traceability methodology aimed at generating specific materials and products such as guides, training activities and technical positions, with visibility, impact and shared use.

In this regard, the following actions are proposed:

4.1. Structured cooperation with privacy professionals and DPOs, their representative organisations and associations will be strengthened in order to consolidate an active community, especially in the public sector, following the best practices of regional authorities with a view to the exchange and joint development of good practices. Regular sectoral meetings will be held and the review of the DPO channel and the improvement of the current certification scheme will be promoted, ensuring its practical usefulness and consistency with professional needs.

4.2. A strategy will be followed to consolidate the role of the DPO, strengthening their functional independence and capacity to act. Proposals will be addressed to clarify the legal status of the DPO, including possible incompatibilities with functions such as information security, IT, regulatory compliance, AI managers or reporting channels.

4.3. Links with regional data protection authorities and other relevant bodies and authorities in related areas, such as AI, cybersecurity, justice, education and digital health, will be strengthened. The joint development of guidelines, standards, technical criteria and training and awareness-raising activities will be promoted.

4.4. In the field of education, the creation and incorporation of quality content on privacy, digital rights and data protection will be encouraged in school and university curricula and teacher training, as well as in research programmes and academic collaboration with universities, training centres, CRUE (Conference of Rectors of Spanish Universities) and CSIC (Spanish National Research Council).

4.5. A cross-cutting intervention strategy will be developed targeting vulnerable groups in the digital environment, with a particular focus on the risks of AI, replicating successful models such as those already applied in the field of minors. This strategy will incorporate new specific lines for people with disabilities, older people, women victims of digital violence and migrants, through the development of adapted materials, the updating of guides and the formalisation of partnerships with universities, specialised entities and the third sector.

4.6. Cooperation with ENAC and key actors in the privacy ecosystem will be updated to promote data protection certification schemes —including standards relating to processes, products or services— that encourage the development of recognised seals and independent accreditation schemes in accordance with the GDPR.

4.7. Likewise, collaboration with professional associations and business organisations will be strengthened to promote regulatory compliance and a culture of privacy in the professional and economic spheres.

Area 5. Leadership and international and national strategic influence

The Agency's presence and influence at international level will be planned and strengthened, particularly with regard to the European Union and the European Data Protection Board, as well as its outreach to Latin America, with a special focus on key areas of technological innovation, mutual recognition of certifications and codes of conduct, adequacy decisions and Binding Corporate Rules for international data transfers with guarantees. In this regard, the following objectives are proposed:

5.1. The Agency will consolidate and increase its participation and leadership in the main national and international privacy forums, with special attention to its role in the European Data Protection Board (EDPB). To this end, it will strengthen its institutional capacities, including the support of the Privacy Lab, with the aim of becoming a European and international benchmark. It will also actively promote simplification initiatives at European level.

5.2. The International Relations Division will develop a structured, proactive and assessable international policy, coordinated in particular with the Technological Innovation Division and the Office of the President, based on clear institutional priorities, strategic participation criteria and operational planning by thematic areas.

5.3. The Secretariat of the Ibero-American Data Protection Network (RIPD, by its initials in Spanish) will promote the focus on objectives and results of the working groups, with operational roadmaps and indicators.

5.4. Work will be carried out to consolidate the RIPD website as an international reference repository on data protection and privacy, as well as to give visibility to the results.

5.5. Actions will be coordinated with countries in the region, strongly supporting the updating of the Ibero-American Data Protection Standards and in collaboration with the Ibero-American General Secretariat (SEGIB). Specific standards on AI and privacy will be promoted, as well as the identification of regulatory needs in areas such as neuro-rights.

5.6. A comprehensive map of the institutional ecosystem in Ibero-America and the Caribbean will be drawn up, identifying key organisations such as the OAS, CELAC and the IDB, as well as common interests, possible alliances and specific avenues for cooperation in the strategic context of Spain or the European Union towards Ibero-America.

5.7. Priority will be given to the active presence of the AEPD as an advisor or observer in global initiatives on digital rights, such as the development of the EUDI Wallet or age verification, and contributions will be made to the drafting of technical guidelines within the framework of the EDPB, the DSA or the Neurodata Group.

Area 6. Effective and continuously improving administration

The actions that make up this priority aim to optimise the organisation and its effectiveness, stabilise the Agency in its new headquarters, improve staff well-being and provide it with more resources and greater capabilities, as far as budgetary provisions allow, as a means of enabling the entity to provide better and higher quality services to citizens.

6.1. Efforts will be made to achieve a proportional increase in human, budgetary, technological and infrastructure resources in order to adequately assume the new functions assigned to the Agency as the Supervisory Authority for the AI Market and other emerging regulations such as the Data Regulation, Data Governance Regulation, Health Data Regulation and Political Advertising Regulation, among others, as well as those it already has.

6.2. The Agency will implement a comprehensive talent development and retention plan, which will include specialised ongoing training, flexible working arrangements and teleworking aimed at work-life balance, professional development and regular performance reviews with constructive feedback. This approach will be complemented by specific indicators and actions that reinforce a culture of continuous improvement, internal participation and horizontal accountability.

6.3. The possibility of optimising the length and format of resolutions will be analysed, incorporating textual analysis techniques where appropriate. Likewise, the promotion of alternative courses of action will be assessed, with measures such as warnings or the recognition of rights, where appropriate.

6.4. A technical and preventive assessment will be made of aspects such as the possible concurrence of disciplinary proceedings and the application of mediation, always with a view to effectively improving proportionality and legal certainty in the disciplinary system.

6.5. Collaborative and advanced management of institutional knowledge will be promoted through mentoring mechanisms, communities of practice and recognition of good practices, together with the implementation of an intelligent document and knowledge management system, ensuring that the renewal of staff preserves the experience accumulated within the Agency.

Area 7. Openness, proximity and a culture of data protection

The Agency will reinforce its open, transparent and accessible nature by improving its website, search engine, implementation of tools, customer service channels, clear and proactive communication, and constantly updating its digital presence. It will promote a culture and literacy in privacy and data protection, collaboration with professional sectors and active listening to anticipate emerging risks. Similarly, it will implement mechanisms for accountability and evaluation of its strategic objectives and public awareness of its functions. The following measures stand out within this area:

7.1. Privacy culture and literacy will be promoted as a key preventive tool, promoting inclusive materials adapted to different levels and formats, as well as awareness-raising actions with specialised groups and entities. These campaigns will target both vulnerable groups (children, the elderly, people with disabilities, people affected by gender or sexual orientation, or those affected by AI, among others) and broader social groups (educational, sporting, cultural, festive), including protocols for action against illegal content and resources adapted to each environment.

7.2. A creative strategy will be rolled out to engage with civil society, professionals, organisations and institutions using informal mechanisms such as ambassadors, the AEPD community, flags, educational and university volunteers, as well as public awareness events, promoting informative content generated by the community.

7.3. Practices and protocols for public consultation and dialogue will be established prior to the publication of guidelines and criteria, especially in complex areas such as AI, biometric systems, digital identity and neurotechnologies. This will be complemented by the creation of specialised dialogue spaces focused on the early detection of regulatory risks and conflicts arising from technological innovation, the exchange of good sectoral practices and the joint development of interpretative criteria.

7.4. Regular open sessions will be resumed, in collaboration and with the participation of other relevant actors, in both face-to-face and virtual formats, to present new developments, interpretative criteria and relevant resolutions in open and interactive formats.

7.5. A comprehensive communication strategy will be developed to bring the Agency closer to all audiences, using a clear and informative tone, a stronger presence in the media and social networks, and useful content for professionals, SMEs and the general public. Awareness campaigns will be created to broaden knowledge of the institution's work, highlighting its role in support and prevention.

7.6. The institutional website and the search engine for resolutions, reports and documentation produced by the Agency will be substantially improved, incorporating new smart tools and accessibility criteria. Improvements to website access will be studied and service channels will be simplified, particularly for citizens and SMEs.

7.7. Finally, the Agency's transparency will be strengthened by improving the public agenda, publishing strategic and compliance indicators, and systematically communicating the most relevant decisions. The publication of resolutions, reports and documents of high interpretative value or practical utility will be promoted, even when their dissemination is not mandatory, always ensuring the protection of the rights, interests and confidentiality of the persons concerned. This will include decisions, legal reports, responses to Article 36 GDPR requests, certification schemes or other initiatives.

Continuous evaluation and dynamic review of the Plan

The implementation of the 2025–2030 Strategic Plan is set out in an internal operational document, which translates its 45 strategic objectives into more than 200 specific measures, distributed among all the Agency's functional units. This administrative document is fully practical, executive and assessable in nature. For each measure, it identifies the units responsible, the deadlines, the monitoring indicators, the implementation phases and the expected results, thus constituting the institutional scorecard which, under the coordination of the Office of the President, will guide the AEPD's actions during the Plan's period of validity.

This operational deployment ensures that the strategic objectives are translated into tangible actions that can be adapted to changing scenarios. Implementation will be subject to a continuous monitoring and evaluation system based on specific indicators and integrated into a systematic monitoring system aimed at identifying progress, deviations or needs for adjustment.

In addition, a review and update of the Strategic Plan is planned to allow for the dynamic incorporation of any necessary adjustments in response to new regulations, emerging technologies or changes in the institutional, social or economic environment. This will enable the inclusion of new objectives or lines of action, the reformulation of existing goals and the adaptation of operational measures to the priorities identified at any given time. Public information will be provided on the development of the Strategic Plan, including general analyses of its progress and main results.