



# MEMORY ANNUAL

**2023**

# Foreword

Once again I am pleased to present the Annual Report of the Spanish Data Protection Agency, a document in which you can find the details of the activity carried out by this organization - in all its areas, an analysis of the most notable trends in data protection and a presentation and assessment of present and future challenges.

One of the most important aspects is the contribution that the Agency has made to improve the protection of children and adolescents - as a central and fundamental axis of public policies. The first year of my mandate, in 2015, we created the Agency's Minors Unit, aware of the great challenges we faced - before, and shortly after we created a transversal working group with experts from various areas to analyze the impact that technologies - have in health, education, family and social life, privacy and, in general, for the comprehensive development of minors.

Over the last few years we have launched initiatives that allow - They can respond to exceptionally delicate situations, such as the Priority Channel to request the urgent removal of sexual or violent content published on the Internet without the consent of the people who appear in it. Also in 2023 we have - has continued to launch awareness campaigns and materials, several of them in collaboration with other organizations, so that both families and educational centers are aware of the risks associated with misuse of screens, the Internet and social networks and can - become allies to promote the education and critical spirit of the youngest. Currently we are facing a new turning point to contribute to the development of healthy habits on the Internet, finding ourselves in a multidisciplinary framework and a country project that is especially conducive to making decisions and carrying out public policies that allow us to continue taking steps towards a society - advanced digital security that protects citizens and especially their children.

In this sense, the following pages include a wide variety of awareness-raising, dissemination, collaboration and inspection initiatives - tion. One of the most notable has been the presentation of the age verification system to protect minors from accessing adult content on the Internet. The development principles - lled by the Agency combine the protection of childhood and the best interests of minors with the fundamental right to data protection of all citizens, putting on the table a solution - practical, respectful and pioneering approach in Europe.

The fact of having proposed a mechanism that treats the attribute of age on the user's device, without the identity of the person - sona nor his age is accessible for web pages or for cars - so-called "trusted third parties" guarantees the privacy of adults while preventing the early exposure of minors to content that they are not capable of managing and that affects them - so seriously in their online behaviors, as doctors and pediatricians already point out. Furthermore, the attention that the Agency pays to the protection of minors in the digital sphere has led to the design of a new reinforced strategy that groups together the measures that the Agency is deploying in its 2024 actions.

The actions mentioned above have been launched in parallel to the usual management of the Agency, which can consult - be discussed on the following pages. The previous reports show a quantitative and qualitative increase in citizens' concern for the protection of their data, which is reflected in the vo - number of claims filed with the Agency in recent years and, in particular, the 43% increase in claims - nes presented in 2023 compared to the immediately previous year, exceeding 21,000. Thus, for the third consecutive year, the number of complaints received has been the highest in its history. This situation - tion does not seem temporary and is posing new management challenges for this Agency. Furthermore, this significant numerical increase in the workload is accompanied by greater complexity in its content, largely driven by the advancement of technologies such as biometrics, artificial intelligence or big data. For this reason, it is essential to offer resources and materials from the Agency such as those also launched this year, which facilitate compliance with the regulations for those who process data, as well as the figure of transfer, which allows the person responsible for the treatment to offer a response. more agile for the citizen than opening a procedure would entail. In this sense, it is important to mention the more than 111,000 data protection delegates notified to the Agency, whose preventive and collaborative work contributes to improving the protection of citizens.

On the other hand, it is necessary to refer to one of the most innovative and relevant initiatives in which we are entering: developing proposals to guarantee the treatment of neuro- data within the framework of the right to the protection of personal data. Neurotechnologies allow the processing of neurological data or neurodata and also allow acting on the nervous system.

and, although these could have a different nature, when they are associated with identified or identifiable people they are personal data.

Neurodata shares characteristics with genetic data, since the brain is an identifier as unique as a fingerprint or a genome. For this reason, we are already working to promote the regulatory recognition of the five neurorights proposed at the international level: personal identity, which protects the person's consciousness against external technological data; free will, which preserves people's ability to make decisions freely and autonomously; mental privacy, which protects people from the use of data obtained during the measurement of their brain activity; equitable access, which seeks regulation to increase brain capabilities, so that they do not generate inequality in society and protection against bias, to prevent people from being discriminated against for any factor, such as a mere thought. This area, together with the protection of children and adolescents on the Internet, will be two of the priority areas for this Agency in the coming years.

Every year I end this prologue by thanking the work done by the public employees of this Agency. It is obligatory and fair.

This body carries out work that involves guaranteeing a constitutional right that faces undoubted challenges. I am convinced of the dedication and effort of all the staff since, without these elements, the actions that are included in the following pages would not have been possible. It is an honor to work alongside such a committed, cohesive and willing team to work on the challenges ahead.

Sea Spain Martí  
Director of the Spanish Data Protection Agency

# Index

## Report 2023

▲ <b>1. Main milestones of 2023</b>	eleven
▲ <b>2. Privacy challenges</b>	<b>13</b>
2.1 Legal	14
2.1.1 Queries	14
2.1.2 Mandatory reports	24
2.1.3 Sentences	27
2.2 Technological	42
2.2.1 Personal data breach notification management	42
2.2.2 Prior consultations	42
2.2.3 Help resources: guides and tools	42
2.2.4 Promotion of the development of the digital economy	43
2.2.5 Promotion of scientific-technical research	Four Five
2.2.6 Adequacy of public administrations guides and recommendations	Four Five
2.2.7 International projection in proactive responsibility: european framework	46
2.2.8 Dissemination actions	46
▲ <b>3. At the service of citizens. Protection of people in a digital world</b>	<b>47</b>
3.1 Education and minors	49
3.2 Communication	52
3.2.1 Social networks	52
3.2.2 Other dissemination actions	53
3.2.2.1 AEPD monthly newsletter	53

# Index

## Report 2023

3.2.2.2 The Agency's blog	54
3.2.2.3 Space "We protect your privacy" on Radio 5	54
3.2.2.4 Media relations	54
3.3 Institutional agenda	55
3.4 Infographics	59
3.5 Presentations	60
3.6 Collaboration and dissemination initiatives	63
3.6.1 Support for the proposed State Pact "Protecting children and adolescents in the digital environment"	63
3.6.2 Update videos Protect your privacy: Whatsapp, Instagram, Tiktok	63
3.6.3 Specific dissemination of the Priority Channel and the responsibilities that may be incurred when disseminating sensitive content, and for which their parents may have to respond jointly and severally.	64
3.6.4 Collaboration with the Ministry of Public Function	64
3.6.5 Dissemination of projects with FIIAPP	64
3.6.6 Promotion of the Priority Channel - March 8	64
3.6.7 Collaboration with Eurochild	64
3.6.8 Agreement with RTVE	65
3.6.9 Fourth edition of the online course "Minors and Internet Safety", organized by the AEPD, INCIBE and INTEF	65
3.6.10 MOOC "Educate in digital security and privacy" 2023	65
3.7 Dissemination campaigns	65
3.8 Awards	67
3.9 Access to public information and transparency	70

# Index

## Report 2023

<b>▲ 4. Effective help to entities</b>	<b>71</b>
4.1 Obligated subjects and Data Protection Officers (DPD): operation of the DPD Channel and assessment of the queries of the Data Protection Officers	71
4.2 Registration of Data Protection Officers	72
4.3 Meeting with the DPOs of the AAPP	73
4.4 DPD Certification in accordance with the AEPD-DPD scheme	75
4.5 Codes of conduct	75
4.6 Promotion of the fundamental right to data protection	77
4.7 International transfers	78
<b>▲ 5. The power of supervision</b>	<b>78</b>
5.1 Results	78
5.2 Most relevant claims and procedures	84
<b>▲ 6. A resilient and constantly improving organization</b>	<b>101</b>
6.1 Talent acquisition and commitment to workplace well-being	101
6.2 Advances in digitalization	102
6.3 Efficiency in resource management	105
<b>▲ 7. The necessary institutional cooperation</b>	<b>106</b>
7.1 Advisory Council	106
7.2 Regional authorities	106
7.3 Relations with the Ombudsman	107

# Index

## Report 2023

<b>▲ 8. An active authority on the international scene</b>	<b>108</b>
8.1 European Union	108
8.1.1 European Data Protection Committee (EDPC)	108
8.1.2 Taskforce on competition, consumption and data protection	120
8.1.3 Taskforce on cooperation of EDPB members in other international forums	121
8.1.4 High Level Group for improving the implementation of police and judicial cooperation in the EU	121
8.1.5 High Level Group for the implementation of the European Union Digital Markets Law	121
8.2 Supervision of the IT Systems of Police and Judicial Cooperation of the Space of Freedom, Security and Justice – new Coordinated Supervision Committee	122
8.2.1 Coordinated Supervision Committee (CSC)	122
8.2.2 VIS Supervision Coordination Group (VIS SCG)	123
8.2.3 Eurodac Supervisory Coordination Group (GCS) (fingerprint information system)	123
8.2.4 Participation of the AEPD in other international forums	124
8.2.4.1 Council of Europe	124
8.2.4.2 Global Privacy Assembly (GPA)	125
8.2.4.3 International Working Group on Data Protection in Technology – Berlin Group	125



# Index

## Report 2023

<b>▲ 9. Cooperation with Latin America</b>	<b>126</b>
9.1 RIPD Meeting February 2023	126
9.2 RIPD coordinated action. Artificial Intelligence - ChatGPT	126
9.3 RIPD coordinated action. CoLDH Application	126
9.4 RIPD XX Anniversary Meeting	126
9.5 InterCoonecta 2023 Program of the AECID	127
9.6 SEGIB call	127
9.7 Webinar	127
9.8 Collaborations	128

## The Agency in figures

<b>▲ 1. Data inspection</b>	<b>130</b>
<b>▲ 2. Legal Cabinet</b>	<b>155</b>
<b>▲ 3. Attention to citizens and obligated subjects</b>	<b>164</b>
<b>▲ 4. Technological innovation division</b>	<b>190</b>
<b>▲ 5. International presence of the AEPD</b>	<b>191</b>
<b>▲ 6. General Secretariat</b>	<b>200</b>

## 1. Main milestones of 2023

The 2022 Report, based on the implications that the digital society has generated and, in particular, the business model based on the monetization of users' personal information by Internet service providers, described the main milestones and risks that affected the fundamental right to data protection and the initiatives to guarantee it and promote citizen trust.

thematic, or addictive, of screens, and access to content intended for adults, especially pornography, whose harmful consequences have been revealed, both by organizations defending the rights of minors and their well-being in the digital sphere as well as by large sectors of the population that demand actions to address the risks they entail.



In the Report, one of the main concerns of the current digital environment was highlighted as being related to **access to mobile devices by minors, the time period in which they use them and the Internet services they access.**

That is why the initiatives adopted to respond to this situation occupy a prominent place in this Report.

During the year 2023, the AEPD has had as its priority objective the promotion of the meetings of the Working Group, launched in 2019, for the protection of minors in the digital world "Minors, digital health and privacy", with the aim of addressing those situations of the use of ICT that affect their privacy, well-being and digital health, in short, their integral development as people, since the protection of their data, their privacy is to protect their development.

Minors constitute the group with the highest Internet use, as reflected in all studies and surveys, including that of the National Institute of Statistics (INE) on Internet use in homes in 2023, which indicates that **90% of children under 10 years old use the Internet, a percentage that rises to 98.3% at age 15.**

The Working Group has focused its work during 2023 on two main issues: the problematic use

The data on the time and habits of use of screens and the digital services and applications that it implies, also highlighted by different organizations and associations, are worrying due to the harmful consequences that they can produce and that, in vulnerable people such as minors in full development of their personality, they acquire greater significance.

Recent studies have warned that **the IQ of the new generations is decreasing since the turn of the millennium by an average of between 2.5 and 4.3 points every ten years.**

The literacy level of minors has been affected by their intensive use of electronic devices, which shows a decrease in Spain of 7 points, the same number that we are below the EU average.

The latest PISA report affects the decrease in students' reading comprehension compared to the previous edition in 2018, 3 points in Spain and 11 points within the OECD, and 8 points in mathematics. Being distracted by cell phones means losing half of the knowledge of a mathematics course.

UNESCO, in its GEM (Global Education Monitoring) 2023 Report on technology in education, states that the time that children spend in front of the screen has increased, both for educational purposes and for leisure. This increase in time can negatively affect self-control and emotional stability, and increase anxiety and depression.

These circumstances led the AEPD to propose to the educational administrations in its field of action that they consider the adoption of measures to restrict or limit the use of electronic devices in schools due to the serious harm they cause to the health and academic results of students. minors, in addition to school coexistence. Proposal that has been the subject of attention by educational authorities.

The inappropriate or problematic and addictive use of the Internet by minors has harmful effects that seriously affect their personal development, more specifically their health (physical, mental, psychosocial, sexual); your neurodevelopment; His learning; the acquisition of cognitive measures; family and social relationships; consumption habits; or the monetization of your data.

Furthermore, the overexposure of personal information makes them more prone to risk situations that intensive technology consumption can cause, such as cyberbullying, sexting, or grooming, with consequences that are unfortunately irreparable in some cases.

To address this problem, the AEPD has collaborated and disseminated, through the "Change the plan" campaign and its transfer to the Public Administrations competent in the care of minors and their families, the Digital Family Plan of the Spanish Association of Pediatrics, in which guidelines are offered to prevent, detect and guide families in the face of problematic behaviors and deal with them. Likewise, it has established alliances with organizations that ensure the health and digital well-being of minors, such as the Councils of Official Colleges of Psychologists and Doctors.

Regarding **online access by minors to adult content, especially pornography**, which studies and reports from specialized organizations indicate is being produced at very early ages of 9 years, and on a large scale, at a time when Their cognitive development does not allow them to understand what they are seeing, since their personality is not formed, and it generates important disorders in the conception of sexual relations and the role of women.

In this regard, age verification to access these contents is one of the key elements to provide a safe and healthy Internet environment for minors, for which systems are necessary that do so effectively and fully respect the rights and freedoms of people, in particular with the protection of their personal data and privacy.

The AEPD, after numerous meetings with different organizations and entities, has adopted a decalogue with the principles that **age verification systems** must apply, so that minors do not access these contents without the system knowing any information. that can identify or trace the user. Principles whose application has been successfully tested through **concept tests carried out by the Agency with the main operating systems**.

The decalogue and the proofs of concept, together with **the list of FAQs** that have been prepared for better understanding, were presented on December 14 on the occasion of the 30th anniversary of the AEPD.

The attention that the Agency pays to the protection of minors in the digital environment has led to supporting the initiative for a **State Pact for the protection of minors in the digital environment**, promoted by relevant civil society entities that defend the rights of children and adolescents and the best interests of minors, with which the commitment of all the agents involved is pursued for the adoption of measures in the different areas of action. .

In addition, we have designed **a new reinforced** strategy which has already seen the light in the month of January 2024, in which the measures that the Agency will deploy in its actions in 2024 are grouped around 3 strategic axes of action.

## 2. Privacy challenges

The 2022 Report raised the need to adopt measures that would guarantee a correct interrelation between the European Commission's digital package and, especially, the proposal for an Artificial Intelligence Regulation.

This collaboration will be necessary since the right to privacy and protection of personal data must be guaranteed throughout the life cycle of the AI system, with data protection authorities maintaining their full powers in terms of data protection. personal data about artificial intelligence systems.

In this sense, data protection regulations apply to artificial intelligence systems and, in particular, the principles of **data minimization and data protection from design and by default** when in artificial intelligence systems personal data is processed.

The interrelation between both standards also affects other areas such as risk analysis, **impact assessments** related to the fundamental rights that the AI Regulation establishes as mandatory for systems that it considers high risk, and impact assessments for the data protection or the concept of **informed consent** required in the AI Regulation as necessary to use a person's information in an AI system that is to be subjected to real tests and the GDPR **consent** necessary to process their personal data in the artificial intelligence system.

Both the jurisprudence of the Court of Justice of the European Union (CJEU) and the opinions of the EDPS (section II.5 of the EDPS Necessity Guide) state that the impact assessment of a regulation in relation to data protection must be carried out in cases where the proposed legislative measure involves the processing of personal data. Any data processing operation provided for by law implies a limitation of the right to protection of personal data, regardless of whether such limitation may be justified.

In relation to the impact assessment for data protection in regulatory development, the Agency published guidelines to identify in which cases the impact assessment should be carried out, how it should be carried out if so, identifying the appropriate range of the standard, evaluating the limitations and risks to rights and freedoms, their purpose, suitability and necessity, the proportionality of the measures, as well as the measures that must be considered to overcome the risks to the rights of those affected.

Additionally, it has proposed that all draft general provisions analyze their implications for data protection, including in a provision included in the standard, provisions that facilitate their application in this area.

The relevance that the General Data Protection Regulation (GDPR) attributes to the figure of the Data Protection Officer (DPO) has required active conduct on the part of the Authorities in order to analyze their situation in the public sphere and private sector and propose measures aimed at guaranteeing adequate development of its functions.

In this regard, the Agency has participated in the coordinated European action to carry out the designation and status of Data Protection Officers, which has concluded with a report in which recommendations are made on their designation, knowledge and experience; their tasks and resources and their position within the framework of the organizations in which they provide their services in order to respond to the relevant deficiencies that have been appreciated.

In the same sense, the Agency has promoted meetings with Delegates of Protection of Data from local entities that have made it possible to know their situation and promote good practices in this sector.

Additionally, various reports from the Legal Office have indicated the criteria that must be met regarding the need to guarantee its organizational autonomy, about the resources that allow it to carry out its work effectively, about the requirement to avoid that in the development of the functions it has attributed by the person responsible, a conflict of interest occurs that affects their necessary independence and the circumstances that may arise for their possible removal.

Regarding the implications of data space initiatives, in order to promote higher levels of legal certainty in relation to the processing of personal data, the Agency has published the document [Approach to data spaces from the perspective of the GDPR](#), which includes a description of the applicable regulatory framework, the methodology for identifying the risks that may be generated and the realization of the impact that addresses them, the different agents involved in them and their legal position within the framework of the GDPR and the legal bases and exercise of data protection rights are analyzed, as well as the guarantees for international data transfers.

The AEPD is addressing as one of its most innovative and relevant initiatives the development of proposals to guarantee the processing of neurodata within the framework of the regulations governing the fundamental right to the protection of personal data, in the absence of a regulation. specific information on this matter.

Neurotechnologies allow the processing of neurological data or neurodata and also allow acting on the human nervous system. The neurodata collected through neurotechnologies could be of a different nature. However, as long as they are associated with identified or identifiable persons, they are personal data.

This is why the risks associated with the processing of neurodata require specific attention regarding the interpretation of its processing in relation to the GDPR.

Additionally, it is necessary to promote the normative recognition of the five neurorights proposed at the international level, such as personal identity, free will, mental privacy, equitable access and protection against bias.

Finally, a reference should be made to the fact that the data on complaints submitted that are collected in the Agency's reports in recent years show that the magnitude of the personal data being processed and the constant evolution of the technologies that are used for their processing, show a quantitative and qualitative increase in the concern of citizens that has been reflected in the volume of complaints filed with the Data Protection Agency in recent years and in particular in the increase of 43 % in 2023 compared to the immediately previous year.

The need to continue generating citizens' trust has resulted in the Agency adopting new organizational measures and proposing legislative initiatives to guarantee this fundamental right.

## 2.1 Legal

### 2.1.1 Queries

In 2023, the activity of the Legal Office has focused mainly on the issuance of mandatory reports on legal and regulatory provisions, as well as those other matters of a general nature regarding data protection that, given their relevance, made it necessary to pronounce this institution.

In effect, regarding the preparation of legal and regulatory provisions, we continue to insist on the need for the body proposing the standard in question to carry out and incorporate into it, the risk analysis and, where appropriate, the evaluation of regulatory impact and that said incorporation is made either in the standard itself or through additional provisions, or is incorporated in the regulatory impact analysis report.

This mandate issued by the AEPD is a call to comply with the principle of active responsibility of the data controller, which requires active intervention by the Data Protection Delegate in Public Administrations, through his intervention in the elaboration. ration of general provisions. In short, it is intended that the regulatory provisions incorporate, adapting to the specific case, a specific regulation on data protection.

However, it should be noted that this insistence in past years has not been in vain and currently general provisions have been approved, the projects and preliminary drafts of which were informed by the Legal Office, and which have their own regulations regarding protection. of data.

In this sense, it is appropriate to cite Organic Law 11/2021, of December 28, on the fight against doping in sports, (Fourth additional provision); Law 13/2022, of July 7, General Audiovisual Communication, (DA fourth); Law 20/2022, of October 19, on Democratic Memory, (DA tenth); Law 2/2023, of February 20, regulating the protection of people who report regulatory infractions and the fight against corruption, (Title VI, arts. 30 and 32); Law 3/2023, of February 28, on Employment, (article 16); or Law 7/2023, of March 28, on the protection of the rights and well-being of animals, (article 10, sections 2, 4, 5, 6, 7, and article 12).

On the other hand, the work of the Legal Office stands out in the preparation of Circular 1/2023, of June 26, on the application of article 66.1.b) of Law 11/2022, of June 28, General Telecommunications, for which Reports 40/2023 and 52/2023 were issued. This Circular became necessary after said regulation came into force one year after its approval, on June 29, 2023, and included the right of users not to receive calls for unsolicited commercial communication purposes, unless there was prior consent. of the user himself to receive this type of communications or that these may rely on another basis of legitimacy than those provided for in the RGPD. In the

Circular, among other issues, includes the requirements of consent and addresses a detailed regulation of legitimate interest as the supposed legitimizer of this type of processing, remembering that, in any case, the principle of transparency must be complied with in relation to the right to information of the owner of the data that will be processed.

As for other matters in which the Cabinet Legal has intervened expressing the criteria of the AEPD, it is necessary to cite the following reports grouped by subject:

**Starting with the figure of the Data Protection Officer (DPD) and the data protection policies, it is appropriate to cite Reports 34/2023 and 38/2023.**



In **Report 34/2023**, the Draft Decree of the Consell of the Balearic Islands is submitted to the criteria of the AEPD, approving the General Policy, Organizational Structure and Assignment of functions regarding Data Protection in the Administration of the Consell and its Instrumental Public Sector. It addresses, on the one hand, the nature and content that data protection policies must have and, on the other, the structure in which the figure of the DPD is incorporated.

The report is based on the doctrine on the distribution of powers between the State and Autonomous Communities and the limit of the essential content of the fundamental right to data protection, indicating that the norm submitted to the report "may only regulate aspects derived from the regulatory development and the execution and application of the RGPD and the LOPDGD in its field of activity, without in any case being in accordance with the required range of law (article 81.1 of the Constitution) and the distribution of powers that regulate essential aspects of the content of the fundamental right ."

In view of the content of the projected regulation, it is recalled that what the RGPD requires in relation to data protection policies is the aspect

effective, practical and executive of a set of guidelines, going beyond the reference to the formal aspect of the existence of a document called “data protection policy” where the mere formal reproduction of the articles of the RGPD is carried out and is reduced to a mere declaration of the person responsible’s willingness to commit to regulatory compliance. That is why it is clear that the “data protection policy” should not be a reproduction of the GDPR or only a formal declaration of assumption of regulatory compliance commitments.

And as for the DPD, it is based on the obligation of the data controller, by virtue of its organizational autonomy, to establish the structure that it deems appropriate to guarantee compliance with the provisions of the RGPD regarding the appointment, legal position and corresponding functions. to the DPD, who must have sufficient autonomy and resources to carry out their work effectively.

For this reason, once the functions of the DPD and those departments that are part of the data controller have been analyzed, the report concludes that within the freedom conferred by the self-organizing power of the public administration, nothing prevents it from being determined in the structure that makes up the person responsible for the treatment, other levels or departments that may participate in determining the purposes and means of the treatment and that to a certain extent advise and propose to the person responsible the adoption of the measures they deem appropriate, but they will always have to be perfectly differentiated from those of the Data Protection Officer, in order to prevent them from being confused with the latter’s advice.

Along the same lines, **Report 38/2023** addresses a series of issues related to the legal position of the DPD, remembering that the assignment of other tasks to the DPD must respect, in any case, its advisory and supervisory nature. without involving direct intervention in decision-making regarding the purposes and means of processing, which would affect their independence and imply the existence of a conflict of interest. In this way, the necessary independence of the DPD and the need to avoid

Conflicts of interest prevent him from being assigned direct responsibilities in an area that he will have to supervise and in which he would be subject to instructions from other bodies.

All of this is in line with the criteria of the Court of Justice of the European Union on the legal position of the DPD and the necessary guarantee of its functional independence in the Judgment of June 22, 2022, case C-534/20, Case Leistriz AG v. LH and in the aforementioned Judgment of February 9, 2023, case C-453/21 Case X-FAB Dresden GmbH & Co. KG against FC.

Finally, the report highlights an essential aspect in the relationship between the DPD and the entity it advises and that needs to be clarified, by indicating that “the employer retains the powers granted to him by labor regulations for adequate compliance and control.” of the employment contract, which are only modulated to the extent necessary to guarantee the functional independence of the DPO, being able to exercise them within the respect of said independence and in such a way that it is not harmed and taking into account that, in accordance with article 36.2 of the LOPDGDD, the DPD may not be removed or sanctioned by the person responsible or in charge for carrying out their functions unless they incur fraud or serious negligence in their exercise.” (...) which does not prevent the DPD from being removed or sanctioned in the event of committing fraud or serious negligence in the exercise of his duties.”

The entry into force of the aforementioned Law 2/2023, of February 20, regulating the protection of people who report regulatory infractions and the fight against corruption, has raised several queries regarding data protection that have been resolved. through reports 54/2023, 60/2023 and 77/2023.



Report **54/2023** resolves a query that raises whether the governing body of each or administrative body of each entity subject to said law should be considered

responsible for the treatment in the terms of its article 5.

The report indicates that in the public sector, the status of data controller will correspond to the entity or body required by law and not to its governing body, without prejudice to the fact that in this area it is a frequent practice in the preparation of the records of the processing activities, to identify as responsible for the treatment the superior or managerial body that holds the corresponding powers, thus contributing to facilitating the identification of the administrative body that adopts the corresponding decisions on the processing. processing of personal data and the exercise of the rights of those affected, a practice accepted and followed by this Agency, but without excluding the status of data controller of the corresponding entity or body.

For all these reasons, the correct interpretation of article 5 of Law 2/2023, of February 20, from the perspective of the protection of personal data, requires identifying as responsible for the treatment the entity or body obliged by law to have an internal information system, without prejudice to the fact that the decisions necessary for its correct implementation must be adopted by the corresponding administrative body or governing body.

Report **60/2023** submits to the criteria of the Legal Office the methods and periods of conservation of personal data that have been processed as a consequence of the application of the aforementioned law, and their coexistence with those regulations that provide different possibilities of preserving certain information, such as those derived from article 31 bis.2 and article 31 quarter.1, letter d) of the Penal Code.

From the norm we deduce the existence of two perfectly differentiated spaces with a different regime in qualitative and quantitative terms.

On the one hand, the Internal Information System, where the information conservation periods are a maximum of three months if they have not been

The corresponding actions have been initiated, and, if the actions have been initiated, the deadlines of the "procedure" processed by the obligated subject must be met and that, although it is not expressly indicated in the law, from its precepts it can be deduced, in principle, , which is six months in certain cases article 9.2 d). In any case, whether the actions have not been started or if they have been carried out, once the indicated deadlines have passed, the personal data must be deleted from the system, unless they are kept in an anonymized manner for the purposes of proving the existence and operation of the system, for example, before the Independent Whistleblower Protection Authority.

And, on the other hand, the record book that contains both the information received and the actions carried out, and whose access is more limited, the regulation itself indicates that it is not public, and can only be accessed upon reasoned request by the competent judicial authority, the conservation periods being those strictly necessary to comply with the law, and in any case a maximum of ten years.

Finally, these conservation and deletion obligations would not prevent the person responsible for the treatment, in order to be able to exercise with all guarantees the rights provided for in article 24 of the Constitution, in a hypothetical criminal procedure, in relation to the provisions of the article 31 bis 2 and article 31 quarter 1. d) of the Penal Code, may keep in a space separate and distinct from those derived from Law 2/2023 of February 20, that information that is necessary for this purpose, precisely to comply with the purposes that would justify said treatment in accordance with other laws that also bind them.

Which does not free the person responsible from complying with data protection regulations, in the sense that they will need the corresponding legal basis for another purpose, and in particular they must take into account those obligations related to the transparency of the treatment, such as , include this possible treatment in the Registry of Treatment Activities (article 30 RGPD) and, where appropriate, in the Inventory of Treatment Activities (article 31.2 LOPDGDD), as well as compliance with the principle of minimization,



both in its quantitative and temporal aspects and above all, to analyze and evaluate the risks associated with this type of treatment as deduced from article 28.2 c) of the LOPDGDD.

Finally, Report **77/2023** addresses the possibility of processing personal data that is contained in the information received within the framework of the information procedure of Law 2/2023, and that does not pass the admission process because it is not under its scope of application. But unlike what was resolved in the previous report, its subsequent use does not refer to the exercise of certain rights, but rather to the protection of article 112 of Law 40/2015 of October 1 on the Legal Regime of the Public Sector. The consultant is the Correos State Company and intends to legitimize the use of said information to meet the objective of "pursuing the efficiency, transparency and good governance of commercial companies."

The response of the Legal Office is negative, since said article 112 does not provide, either directly or indirectly, for the interference that it would entail in the fundamental right to data protection and nor does it justify the legal obligation or public interest that would justify data processing, personal data other than that provided for by Law 2/2013 itself, and obviously no guarantees or limits of any kind are established in the standard for the specific treatment that is proposed. The report also analyzes the possible concurrence of a hypothetical legitimate interest as a legitimizing basis to conclude by ruling out this possibility, to the extent that "it is difficult for a hypothetical informant who goes to the internal information system, covered by the law of confidentiality and anonymity notes, can reasonably expect that the information provided can be used for another purpose such as that intended by the consultant."

The report concludes that the new treatment would not find a sufficient legal basis and would have a purpose incompatible with the initial one.

Another aspect with an obvious impact on data protection is the fraud prevention systems, with respect to which Report 18/2023 has been issued this year, which updates the legal regime to which

The Confirma File is submitted regarding several aspects, such as the role that the entities adhered to said system would play and the new types of annotations in relation to compliance with the principles of the RGPD.

**Regarding the principles of data protection, the principle of legality is addressed in Reports 7/2023 and 70/2023 and which refer to the legal bases that legitimize the requests made by authorities and that imply processing . of personal data.**



Report **7/2023** analyzes the request for information made by the General Directorate of Gambling Regulation (DGOJ), of the General Secretary of Consumption and Gambling, of the Ministry of Consumption, to the Royal Spanish Football Federation (RFEF) to the protection of Law 13/2011, of May 27, on the regulation of gaming (LRJ).

The RFEF considers that complying with the information requirement may contravene the RGPD since it could be contrary to the principles of legality, purpose and minimization.

The requirement refers to "the identification of all members who, as of the date of response to this requirement, are 18 years of age or older and who are part of the management team, player team and technical team (coach, assistants, kit players...), of the sports entities assigned to the five groups of the Second Football Federation category during the 2022/2023 season. Said information, which must be reported in Excel format, will contain at least the following: Team, Group, Name and Surname, NIF, License, Address and location, Type of relationship (player, coach, manager...)"

The report indicates that the requirements under analysis are not made due to a legal obligation applicable to the data controller, the DGOJ, but are carried out in the exercise of the powers attributed to it by articles 21 and 24 of the LRJ in relation to article 6.2 of the same standard.

Consequently, the processing of data derived from the request made by the DGOJ to the RFEF finds its legitimization in article 6.1 e) of the RGPD and article 8.2 of the LOPDGDD, being the norm that attributes jurisdiction to the LRJ.

From the perspective of the RFEF, meeting the request and, therefore, the data processing derived from it finds its legitimacy in article 6.1 c) of the RGPD and article 8.1 of the LOPDGDD, in line with the generic duty of collaboration that emerges from article 18 of Law 39/2015 of October 1, on the Common Administrative Procedure of Public Administrations.

Regarding the principles of minimization and limitation of the purpose, the criterion shown in other reports on the requirements of certain supervision and control bodies to those bound by the standard that applies to them is brought up - State Administration Agency Tax (for all Reports 369/2015 and 98/2016), the Spanish Agency for Medicines and Health Products (Report 59/2021), the Court of Accounts (Report 28/2022) at the regional level, the Audit Office of Balearic Islands (37/2022) - the general criterion being that the delimiting element is the usefulness of the requirement, in the sense of whether it is useful to fulfill the purpose derived from the precepts that attribute the functions and powers to said organizations. In other words, if the data that is going to be processed has significance in relation to the purpose pursued.

And the specific characteristics that these requirements must have (Report 59/2021 and STC17/2013) are recalled: (i) indiscriminate and massive access to personal data must be avoided (ii) the data in question requested must be relevant and necessary (iii) for the purpose established in the precept (iv) the request for access to the specific personal data must be expressly motivated and justified, (v) in such a way that it enables its control by the assignor (vi) and is Avoid tortuous use of this faculty with massive access. This means (vii) that the possibility of analyzing whether in each specific case the access was protected by the provisions must be guaranteed.

established in law. After the exhaustive analysis, the report concludes that the DGOJ requirements made to the RFEF are in accordance with the principles of legality, purpose limitation and minimization.

In **Report 70/2023**, a joint consultation is proposed by the Data Protection Delegates of the Bank of Spain (BE) and the State Tax Administration Agency (AEAT), referring to the possibility that in the collection procedure -and specifically by exercising the possibility of postponement or installments- instructed by the AEAT may request from the BE the report from the Risk Information Center of the Bank of Spain, CIRBE, which refers to the person obliged to pay in said procedure, in relation to What would be the legal basis for legitimization of said data processing.

The report indicates that a hypothetical access to the CIRBE report would be based on article 6.1 e) RGPD and article 8.2 LOPDGDD, as it refers to the exercise of its own powers that are necessary to fulfill a mission of public interest, and not on the consent of the interested party as proposed by the consultants, even though article 46.3 c) of the General Collection Regulations provides for an open clause in which the contribution of the CIRBE report could be included by indicating that in the request for postponement or fractionation must be accompanied by: c) other documents or supporting documents that the interested party deems appropriate. The existence of this faculty in the interested party does not eliminate the existence of a relationship of subjection that prevents free consent.

Secondly, the application of article 28.2 of Law 39/2015 of Law 39/2015, of October 1, (LPACAP) is addressed to legitimize a hypothetical access, since the consultants present it as a legal obligation. The report rejects this approach and reiterates that the administration's action as a consequence of the application of article 28.2 LPACAP, in terms of data protection regulations, is carried out under article 6.1 e) of the RGPD and not in compliance with a legal obligation of article 6.1 c) RGPD.

However, the report concludes that, “for the specific treatment, in coherence with the regulation of the Law of Reform Measures of the Financial System on the CIRBE, the existence of the authorization of the interested party, not consent, should be proven. to which the data protection regulations refer - and the legal basis that will legitimize the AEAT to access the CIRBE report will be that provided for in article 6.1 e) of the RGPD. And it emphasizes that both the contribution of the information contained in the CIRBE by the interested party to the AEAT, and the aforementioned authorization, must arise from the free disposition of the interested party who, in coherence with the LMRSF, is the only holder of the right to access and whose exercise is obviously voluntary. (...) the interested party must freely decide to give authorization to access said data, without the need to be induced, suggested or “reminded” to do so. (...)”



**Regarding special categories of data, reports 41/2023 and 55/2023 stand out, addressing access to medical history.**

In **Report 41/2023**, a series of issues related to the legitimacy for the processing of personal data are resolved through the exchange of information from the medical history of workers between doctors of the public health service (SPS) and doctors of the Mutual Insurance for Work Accidents.

The report, after analyzing the requirements to process special categories of data and the doctrine of the Constitutional Court in this regard (STC 76/2019 of May 22), addresses the legislation that regulates the health treatments to which the consultation refers, starting from the art. 71.3 of the consolidated text of the General Social Security Law, approved by Royal Legislative Decree 8/2015, of October 30, (TRLGSS).

It is recalled that the Agency in its reports 39/2022 and 42/2022, relating to the draft regulatory provisions that develop said precept, considers that the Administration

of Social Security, as it is able to collect the medical history of workers for these purposes, and is regulated by Law 41/2002, of November 14, the basic regulator of patient autonomy (LAP), and is subject to safeguards and guarantees. established in law 41/2002 for its use. This consideration would allow us to overcome the circumstance that art. 71.3 TRLGSS does not establish, in itself, these guarantees for the processing of personal data carried out to fulfill these purposes.

To which he adds that Report 101/2019 already analyzes the possibility that, by the Medical Inspection services of the Autonomous Community of the Canary Islands, medical records of both primary care and specialized care can be accessed. purposes to carry out its functions of verification, control, confirmation and extinction of temporary disability and therein a special analysis is made of the guarantees contained in Law 41/2002.

Therefore, once the legal framework applicable to access to medical records in temporary disability procedures has been analyzed, reference is made to the legal nature of mutual insurance companies and their condition in relation to the processing of personal data, based on the article 80 of TRLGSS.

Affirming that the legitimation for the proposed treatment would be found, as the legislator has expressly recognized in articles 6.1. e) and 9.2 h), of the RGPD Now, said legitimation does not allow an exchange of the information that is part of the medical record as intended in the consultation, since health data processing must be carried out in the terms and with observance of the specific limitations and guarantees included in the legal regulations that legitimize them, which have not provided for such generalized exchange, granting access to medical records, in general, to the managing entities and the medical inspection. And it is noted that treatment such as the intended one could also be contrary to the principles set out in article 5 of the RGPD. In this sense, there are already precedents of sanctions imposed by this Agency as a consequence

of the violation of said principles in cases analogous to the one raised, such as PS/00262/2021, in which a medical center was sanctioned that provided a health insurance company with health data prior to carrying out the test that it had carried out at the request of the mutual, for violation of the confidentiality principle of article 5.1.f) of the RGPD.

A different issue is when, taking into account the circumstances of the specific case, there is a link and that access occurs through the Medical Inspection Service, as reasoned in the Judgment of the National Court of September 20, 2020 (Appeal 186 /2019).

The purpose of **Report 55/2023** is to ensure that the Occupational Risk Prevention Service of public employees of the Public Administration of the Region of Murcia can access their medical records in order to carry out different activities. .

The report begins by differentiating the work medical history and the "ordinary" medical history and the purposes pursued by each one. To then analyze the national and regional regulations that regulate access to medical records, concluding that, "in general, the purpose of the use of medical records responds to the healthcare function that primary and specialized care doctors carry out." . Outside of this purpose, the different uses or exceptions provided for in the aforementioned regulations are listed (sections 3 and 5 of article 16 LAP and sections 4 and 5 of article 55 of the regional law) and none of them identify the Security Services. Occupational Risk Prevention as potential recipients of it. To which we must add that the processing of health data from the medical history must respect privacy, confidentiality and the protection of personal data and any access to said information must be provided for by law." However, it is recalled what is indicated in Report 362/2010 in which it is stated that "On the other hand, the limitations established by the aforementioned article 16 do not necessarily imply that the data from the clinical history can only be accessed in the assumptions listed there, but that an assignment could be admissible if there is another norm with the rank of Law that the

enable. ", so the regulations applicable to the Occupational Risk Prevention Services are consulted, to see if they include the treatments proposed by the consultant and that necessarily involve access to the ordinary or conventional clinical history. . The answer is negative and it is added that if the consultation proceeds as intended "we would be faced with the hypothetical case in which a person goes to the doctor for a specific purpose and subsequently, that information would be used by the Prevention Services of said patient's employer. even in the event that he, in his work environment, had declined the option of undergoing a medical examination. No expectation of privacy or predictability of the treatment would make the owner of the data form when he or she attends a consultation or a specific test in relation to the subsequent treatment that the consultant intends."

The report concludes that the data processing analyzed "does not comply with the principle of legality because it results in a processing of special categories of data without observing the provisions of articles 9 and 6 of the RGPD (...) and would also be contrary to and incompatible with the purpose of the initial treatment. Therefore, the principle of limitation of purpose is not met either."

It is also worth highlighting Report 43/2023 which, although it does not deal with special categories of data, focuses on the possible processing of data of a criminal or police nature and administrative infractions, which have a special processing regime.

The consultation asks whether the communication of data relating to police records of the parents of minors to the technical teams of the competent Administration for the purposes of assessing whether there may be a social risk for minors complies with the regulations on the protection of personal data. the minor or a situation of helplessness.

It is considered necessary for the communication of said data to proceed, in addition to it being provided for by European Union Law or by Spanish legislation, which is assessed if not

The purposes for which the data are kept in police files are harmed or the specific guarantees established by Organic Law 7/2021 are distorted.

Consequently, it is analyzed whether the proposed treatment is contemplated in a norm with the force of law that contains specific guarantees. The answer is affirmative when resorting to the provisions of article 22 quater of Organic Law 1/1996 of January 15 on Legal Protection of Minors, which includes the safeguards proposed by the Legal Office itself in the report issued following the processing of the legislative modification that introduces the precept (Report 195/2014) and it is indicated that said regime of guarantees is also complemented by the generic duty of reservation included in article 13.3 of the aforementioned Organic Law.

Now, the report concludes that “the legal provision of art. 22 quater of Organic Law 1/1996 does not imply a generic authorization for the communication to the autonomous administrative authority of all the personal data that may appear in the police files regarding the parent of a minor involved in a procedure for possible declaration of the situation of helplessness, but only those data that are strictly necessary within the procedure processed by the autonomous authority for the adequate protection of minors by the public powers through the prevention, detection and repair of risk situations, with the exercise of guardianship and, in cases of declaration of helplessness, for the assumption of guardianship by operation of law.

(...) the request for such data by the competent Administration may only be carried out when there is a proven situation of risk of social exclusion or helplessness of the minor, which must be sufficient and expressly motivated and reasoned by the requesting Administration. (...) and will be subject to the principle of minimization (...) without protecting massive transfers of data, being limited to the data necessary to determine the measure or measures that are in favor of the minor in a situation of exclusion or risk. to be applied.(...) and

strictly to the principle of purpose, without forgetting the proactive responsibility regime that will imply that the administration receiving the information "must guarantee the application of the technical and organizational measures that result from the corresponding impact assessment on data protection, in the terms provided for in article 3 of Royal Decree 311/2022, of May 3, which regulates the National Security Scheme.”

Another report that deserves special attention due to the nature of the owners of the data being processed, that is, minors and the context, digital platforms in the educational field,

**is Report 50/2023 that is issued following the consultation of the Ministry of Education, Vocational Training, on the adaptation to the current legal framework of the Agreement between INTEF (National Institute of Educational Technologies and Teacher Training) and Google for the use of the “Workspace for Education” tools in the Educational Centers of Ceuta and Melilla.**



The report analyzes several issues, some strictly referring to the right to data protection, and others that, although they deal more with issues related to civil law, referring to the validity and requirements of contracts, will have an impact at least indirectly in the application of data protection regulations.

Starting with the latter, the report highlights the lack of information in the contract on essential aspects and rejects the circumstance that it is necessary to go to different websites so that the person responsible knows fundamental elements referring to the object of the contract, what the services that are part of it, the type of data that is collected or the details of the purposes that are pursued.

Likewise, it is made clear that the Agreement allows the specific services of the supposed data processor, Google, to be modified, and that the interpretation of the agreement with regard to data protection is subject to a changing document at the will of Google.

Also when analyzing the purposes of the treatments, it is observed that several respond to purposes specific to the person in charge of the treatment, and that they move away from the purpose of offering students the possibility of acquiring digital skills in the educational field. This issue has important consequences when determining the legal basis that legitimizes the treatments, since if they serve a purpose specific to the person in charge, they can no longer be supported by the legal basis of article 6.1 e) and, where applicable, section c) of the RGPD, which legitimizes the processing of data in digital environments by the educational administration for educational purposes.

These aspects are essential to question Google's role in providing the contracted service to the educational administration as a simple data processor, but rather the role it plays is closer to the figure of a data controller. The report also rejects certain clauses on the application of the GDPR and on the choice of subprocessor as confusing and contrary to the current legal framework.

Finally, the report sets out the elements that the data controller must take into account to assess compliance with the principle of proportionality, in relation to the risks assumed, data minimization and privacy by design and by default.

For all of the above, the signing of the agreement by the educational administration is reported unfavorably.

Report **49/2023** responds to a query raised on the occasion of the 50th anniversary of the terrorist attack perpetrated against the then President of the Government and regarding the request for access to the Summary prepared for this purpose by a production company with the purpose of illustrate a television documentary series.

After analyzing the regulations applicable to judicial files, determine that the person responsible for the treatment is the court or tribunal that conducted the summary, and that in accordance with the STJUE March 24, 2022 (case C-245/20), in relation to the access of journalists to personal data that appear in a judicial file, and its section 34, which broadly interprets the concept of "processing "for jurisdictional purposes" contained in article 236.bis of the LOPJ, it is estimated that said processing would fall within the powers that article 236.octies of the LOPJ attributes to the General Council of the Judiciary and not to the AEPD.

However, the report sets out the criteria that have been applied in similar cases in relation to the processing of personal data corresponding to personal data of judges, magistrates, forensic doctors and other officials present in various judicial cases, ( Report 44/2019), in the sense that "the processing of personal data of public officials, in certain cases referring to their exercise and not to information about their private life and in the framework of a historical investigation, could be of general interest, its publication being reinforced by the right to information and the right to freedom of expression." It also rules on the appropriateness of assessing the existence of data referring to criminal convictions and infractions (articles 10 of the RGPD and 10 of the LOPDGDD), all of this in relation to the provisions of article 57.1 c) of the Heritage Law. Spanish History, and the ways to access it depending on whether those affected are alive or not, and the deadlines that would apply.

Report **66/2023** resolves the query regarding how to proceed in those cases in which access to the General Archive of the Ministry of the Interior is requested to exercise the rights it confers.



Finally, it is worth mentioning the following reports that deal with the processing of personal data derived from access to judicial archives and historical archives.

Law 20/2022, of October 19, on Democratic Memory (LMD), in the sense of whether it is said norm that prevails or Law 16/1985, of June 25, on Spanish Historical Heritage (LPHE) which refers to that in some of its precepts.

The consultant maintains that, in practice and in application of the LPHE, she chooses to anonymize the information she provides to access applicants, in response to which she receives numerous complaints because they understand that the information thus provided prevents the effective realization of their rights.

The report indicates that the person responsible for the file must weigh up whether, strictly applying the LPHE and specifically Decree 1708/2011, of November 18, (RDSEA) in its article 28.4 on anonymization, when resolving the requests for access to documents ex article 6 LMD, the right of a person to prove their status as a victim may be affected in such a way that its effective realization is prevented if said anonymization of third party data were carried out.

All this because there is an obvious difference between the access referred to in art. 27.2 LMD intended by people who are potential holders of the right of article 6 LMD to be considered "victims", of the rest of the people who want general access to documents on the coup d'état, the War and the Dictatorship for different reasons. .

The report maintains that "a generalized practice of anonymization based on the normative referral of Article 27.3 LMD, without analyzing the content of the requests on a case-by-case basis, could de facto make impossible or hinder the exercise of the right expressly recognized by the article 6 of the LMD."

Therefore, with respect to said applicants, the report concludes that the principle of regulatory specialty can be applied, and the information cannot be anonymized no matter how much Article 28.4 of the RDSEA allows, and consequently provide the requested information in its entirety as as provided in said *article in its section 2*.

## 2.1.2 Mandatory reports

The AEPD has continued working on the objective of achieving greater legal certainty through mandatory reports on general provisions, aimed at improving the systematics of the legal system by integrating a transversal norm with sectoral regulations. Among the reported provisions it is worth mentioning the following:

- Preliminary Draft Organic Law that modifies LO 6/1985, of July 1 of the Judiciary, the Criminal Procedure Law and Law 23/2014, of November 20, on mutual recognition of resolutions.
- Draft comprehensive Organic Law against trafficking and exploitation of human beings.
- Draft Organic Law on equal representation of women and men in decision-making bodies.
- Draft Industry Law.
- Draft Law on basic conditions for equality in access and enjoyment of social services.
- Preliminary draft law amending the consolidated text of the Law on civil liability and insurance in the circulation of motor vehicles, approved by Royal Legislative Decree 8/2004 of October 29.
- Draft Royal Decree approving the Regulation of the State Registry of Consumer and User Associations.
- Draft Royal Decree that modifies Royal Decree 390/2021 of June 1, which approves the basic procedure for the certification of the energy efficiency of buildings.

- Draft Royal Decree amending Royal Decree 1799/2003, of December 26, which regulates the content of the electoral lists and copies of the electoral roll.
- Draft Royal Decree that develops the composition and operation of the Second Section of the Intellectual Property Commission.
- Draft Royal Decree amending the Regulation of public hydraulic domain approved by Royal Decree 849/1986, of April 11 and the Regulation of public water administration, approved by Royal Decree 927/1988, of July 29 .
- Draft Royal Decree approving the Statute of the Independent Authority for the Protection of Informants.
- Draft Royal Decree establishing the regulations for the youth cultural bonus.
- Draft Royal Decree that modifies Royal Decree 1051/20136, of December 27, which regulates the system benefits for autonomy and care for dependency, established in Law 39/2006 , of December 14, on Promotion of Personal Autonomy and Care for people in a situation of dependency.
- Draft Royal Decree that creates and regulates the State Public Health Surveillance Network.
- Draft Royal Decree regulating the admission of students to public and private centers, within the scope of management of the Ministry of Education and Vocational Training of the cities of Ceuta and Melilla.
- Draft Royal Decree creating the State Agency for Digital Administration and approving its statute.
- Draft Royal Decree amending the Regulations governing private driving schools, approved by Royal Decree 1295/2003 of October 17, and the General Regulations for drivers, approved by Royal Decree 818/2009 of May 8.
- Draft Royal Decree that modifies Royal Decree 1110/2015, of December 11, which regulates the Central Registry of Sexual Offenders.
- Draft Royal Decree relating to the management of waste from tobacco products with filters and filters marketed for use with tobacco products.
- Draft Royal Decree to modify Royal Decree 928/1998 that approves the General Regulation on procedures for the imposition of sanctions for social infractions and for the liquidation proceedings of the SS and RD138/2000 approves the Regulation of organization and operation of the Labor and SS Inspection in matters of digital Administration.
- Draft Royal Decree regulating the financial aid established in art. 41 of Organic Law 10/2022, of September 6, on the comprehensive guarantee of sexual freedom.
- Draft Royal Decree regulating medical devices for in vitro diagnosis.
- Draft Royal Decree modifying article 9 of the Weapons Regulations, approved by Royal Decree 137/1993, of January 29.
- Draft Royal Decree approving the intellectual property registration regulations.



- ÿ Draft Royal Decree regulating the State Registry of audiovisual communication.
- ÿ Draft Royal Decree amending Royal Decree 1082/20212, of July 13, approving the Regulation for the development of Law 35/2003, of November 4, on Collective Investment Institutions .
- ÿ Draft Royal Decree regulating the Democratic Memory Council and the State Registry of Democratic Memory Entities.
- ÿ Draft Royal Decree establishing a controlled testing environment for testing compliance with the proposed Regulation of the European Parliament and of the Council, establishing harmonized standards on AI.
- ÿ Draft Royal Decree amending the Population Regulations and Territorial Demarcation of local entities, approved by Royal Decree 1690/1986, of July 11.
- ÿ Draft Royal Decree Transposition of EU Council Directive 2021/514 of March 22, 2021, which modifies Directive 2011/16/EU on administrative cooperation in the field of taxation, and other tax regulations .
- ÿ Draft Royal Decree approving the Regulation regarding administrative smuggling offences.
- ÿ Draft Royal Decree regulating the certification procedure and continuous supervision of civil providers of air navigation meteorological services.
- ÿ Draft Royal Decree regulating the Public Bankruptcy Registry.
- ÿ Draft Royal Decree that modifies Royal Decree 95/2009, of February 6, which regulates the system of administrative records to support the administration of justice.
- ÿ Draft Royal Decree Carbon footprint registration.
- ÿ Draft Royal Decree developing the Bankruptcy Administration Regulations.
- ÿ Draft Royal Decree modifying Royal Decree 183/2004, of January 30, which regulates the individual health card. \*
- ÿ Draft Consell Decree approving the general policy, organizational structure and assignment of functions regarding data protection in the Administration of the Generalitat and its Instrumental Public Sector.
- ÿ Draft Decree of the Government of Aragon approving the Data Protection and Information Security Policy of the Administration of the Autonomous Community of Aragon. \*
- ÿ Draft Ministerial Order approving the Security Policy of the Ministry of Justice.
- ÿ Draft Ministerial Order regulating the registration of waste production and management.
- ÿ Draft Ministerial Order that develops various provisions of RD 36/2023, of January 24, which establishes a system of Energy Savings Certificates.

- ÿ Draft Ministerial Order creating within the scope of the General Administration of the State, the Safety Registry of dams and reservoirs.
- ÿ Draft Ministerial Order regulating the duration, content and requirements of safe and efficient driving courses, the completion of which entails the recovery or bonus of points, as well as the certification and control mechanisms.
- ÿ Draft Ministerial Order regulating the administrative procedure for the acquisition and loss of the status of entrepreneur service point.
- ÿ Draft Circular on the application of article 66.1.b of Law 11/2022, of June 28, General Telecommunications.
- ÿ Proposal for a Circular regulating the procedure for the supply and reception of subscriber data, in accordance with article 8.2. i of the Organic Statute of the CNMC, approved by Royal Decree 657/2013, of August 30.

### ÿ 2.1.3 Sentences

The analysis of the degree of legal certainty in the application of data protection regulations requires considering the extent to which the AEPD Resolutions are ratified or revoked by the Courts.

This section includes, on the one hand, the Judgments of the National Court, which is the judicial body competent to hear the appeals filed against the resolutions of the AEPD, and, where appropriate, the Judgments of the Supreme Court that hear the appeals of cassation that are filed against the Sentences of the National Court. And on the other hand, it includes the jurisprudence of the Constitutional Court and the European Courts that deal with the matter and that deserve to be highlighted due to their interest.

**During the year 2023, 43 resolutions have been issued by the contentious-administrative Chamber of the National Court, of which:**



- ÿ 24 appeals against Agency resolutions were rejected (which were fully confirmed);
- ÿ 1 partially upheld the appeal;
- ÿ 7 fully upheld the claims to annul the Agency's resolutions;
- ÿ 11 appeals filed against Agency resolutions were inadmissible.

For its part, the **Supreme Court issued two resolutions**, one of which confirmed the criteria of the AEPD and the other upheld the claims of the recurring.

Regarding the sectors of activity of the appellants both in the National Court and in the Supreme Court, of 63 resolutions that resolve appeals against the resolutions of the AEPD, and, where appropriate, against Judgments of the National Court that confirm the resolutions of the AEPD, most of them have been filed by individuals (42).

However, a high number of them are rejected, the most common reason being the lack of evidence or factual and legal inconsistency of the complaint, which advises against even initiating investigative actions, as the court also appreciates.

As in the previous exercise, a good number are specified in which the ruling is the declaration of inadmissibility of the appeal due to lack of active standing because the court a quo is requested, not only the revocation of the resolution. of the AEPD but the imposition of a sanction, the Chamber recalling the absence of a subjective right in that sense for individuals, reiterating the doctrine that the *ius puniendi* is not in the hands of individuals.

Likewise, among the rejections, it is appropriate to mention those that deal with the exercise of rights, both those referring to the right of access in general, as well as those referring to the suppression of police records and that confirm the criteria of the AEPD in that considers that the person responsible has given a valid response in law to the owner of the personal data, being a different matter that said response does not satisfy the particular interests of the affected person, and those in which the emphasis is placed on the formal requirements of the request for the right. or in its repetitive nature.

Individuals are followed by those resolutions referring to the health sector (4), the energy sector (3) and, to an equal extent, the Telecommunications, Banking-Insurance and Associations-Unions sectors (2) and finally the sector of Information Society (1).

## Of the matters analyzed by the Court

### National highlights the following issues:

Starting with those resolutions that deal with the principles related to data processing, such as legality and integrity and confidentiality (article 5.1 a) and f) of the RPDG), the **Judgment of January 27, 2023**, issued in Appeal No. 543/2020 that rejects the claims of the appellant in a case referring to the **provision of personal data to judicial processes**.

The appellant's partner was immersed in a civil process to create an inventory of the matrimonial property regime, in which the representation of the former spouse, through the court, requested from the bank the extract of the accounts "in the name of" that.

When providing said information, the banking entity also incorporates into the case the personal data of the appellant where he was the owner and his partner was listed only as an authorized person.

A possible violation of the principle of legality and confidentiality is analyzed and it is concluded that the treatment found legitimacy in article 6.1 c) of the RPDG in terms of the protection of the provisions of article 118 of the Spanish Constitution and article 17 of the Organic Law. of the Judicial Branch, there was an obligation in the banking entity to comply with judicial requirements. The title of that account was irrelevant in relation to the bank account, since appearing as authorized, it was an account that "existed in his name."

Finally, regarding the principle of confidentiality, the Chamber maintains that the possible dissemination of the appellant's data was "very limited," highlighting the duty of secrecy of the officials of the administration of justice and the other party involved in the process that You have the duty of confidentiality. For all these reasons, the appellant's claims are rejected and the AEPD's resolution of inadmissibility is confirmed.

Continuing with the principle of confidentiality, in the **Judgment of January 9, 2023**, issued in Appeal No. 433/2020, which rejects the claims of the appellant in a case referring to the **publication of data on bulletin boards in communities of owners**.

A claim is filed against the Administrative Secretary of the Community of Owners for publishing a call for the Ordinary General Meeting of Owners on the bulletin board of the building portal where a debt associated with the appellant's home was recorded.

The AEPD resolution focuses its arguments on the fact that, in general, it is not necessary that, within the Community, the owners consent to the use of their own personal data and in relation to late payment, articles 16.2 and 19 of the Horizontal Property Law enable the inclusion of the identifying data of the debtor owners in the Meeting's Calls and in its Minutes. Likewise, the call was posted in a place that is not locked, specifically on a board on the wall of the property's portal. This circumstance is decisive to the extent that the alleged person responsible for the reproached conduct cannot be identified, nor could it therefore be assessed whether the prior requirements for notification to the publication of the accounting situation of the affected party have been met. In this sense, it must be taken into consideration that the exhibition of the document in an open place would allow a plurality of people to carry out the claimed conduct. To which it must be added that only the identification of the property is published in relation to the debts, but not the data of its owner, so (...) this Agency could only come to know about this matter in the event that the documentation provided made it possible to prove that the affected owner is identifiable, a circumstance that is also not appreciated from the documentation provided and on file in the analysis file (...).

The appellant invokes a violation of article 9 of the LPH, given that there is no prior attempt to notify the address and article 5 of the LOPDGDD referring to the confidentiality of the data.

The Chamber rejects the appellant's arguments, recalling the criterion upheld in these cases in its Judgment of March 17, 2011 (Appeal No. 2015/2019) and January 24, 2020 (Appeal No. 597/2017) on the possibility of publishing the call on the bulletin board of the community building (...) stating the existence of a debt of one of said community members in the way in which it was done, since ultimately said fixation of the amount owed is legally protected and constitutes a topic of interest for said Community, and since the debtor is not identified as such, contrary to what is invoked in the lawsuit, it is not accessible to third parties or visitors(...)

---

For its part, the **Judgment of April 28, 2023**, issued in Appeal No. 409/2021, analyzes the adequacy of the **principle of integrity and confidentiality**, when addressing the appeal filed by a **union of civil servants** that is sanctioned by the AEPD.

The facts are that the (...) union delegate (...) has published a list of the census in an open WhatsApp group in which almost all the workers of the Central Radiodiagnosis Unit of the Community of Madrid are located. electoral campaign of exclusive advertising for the unions, including data such as name and surname and ID of all voters who make up the statutory staff, (...)

The sanctioned party states that it has legal protection for said publication, however, the AEPD in its resolution argues that: This legal protection is not found in the Workers' Statute, art. 74, since the way it has been done by publishing the data through an open WhatsApp group is not advertising that is included in that art. 74 ET. (...), likewise, RD 1844/1994 that approves the Regulation of elections to representative bodies of the company's workers (...) there is no legal basis for the publication of the data in the form in which it has been done by giving names and surnames and ID through WhatsApp. Who has the answer?

The ability to publish the census is the Electoral Board and it is a publication that is made through the notice board so that it can be endorsed by voters in order to rectify errors.

The union delegate illicitly processed these personal data by revealing the DNI of the members of the WhatsApp group, therefore there is a violation of art. 5.1.f GDPR in relation to art. 6.1 (...) Freedom of association has been considered in the resolution, and it states that the Freedom of Association Law in art. 8.1.c provides that workers affiliated with a union may, within their company or workplace... c: Receive the information sent to them by their union. And in accordance with the same precept section 2.a: in order to facilitate the dissemination of those notices that may be of interest to union members and workers in general, the company will make a notice board available to them...". But freedom of association is respected and materialized by giving the information in the manner provided for without having to resort to that WhatsApp medium that contributes nothing to freedom of association.

The Chamber concludes that (...) the publication by the CSIF union representative in an open WhatsApp group of the DNI of the workers who formed it was not carried out within the framework of the exercise of the functions inherent to freedom of association, since the publication by WhatsApp of this personal data does not have any union interest. It is a list of the electoral census in which a DNI appears when it is legally provided for in the Workers' Statute, art. 74, that the list of voters will be made public through the notice board through its display. RD 1844/1994 also establishes that the list of voters and eligible voters will be made public on the notice boards. RD 1846/1994 of September 9, art. 14, indicates that in this census the name and surname will be recorded...

DNI, and it is a list that will be made public on the notice boards.

In short, sector regulations provide for the publication of this data on bulletin boards, but of course its publication through WhatsApp, an instant messaging application that can be considered part of the new communication technologies, is not contemplated. that can be used to communicate

information to workers, but due to its characteristics it does not provide security to the confidentiality of personal data. Nothing prevents the union from using these mechanisms such as WhatsApp or similar, but in no way can the use of this instant messaging be accepted automatically for the publication of personal data as relevant as the DNI and whose publication has no relationship with the right to freedom of association, with the right of workers. The content of WhatsApp affects all or almost all of the workers of the Central Radiodiagnosis Unit of the CAM, whether or not they are affiliated with the CSIF, other unions or none, and of course the publication of the DNI of those affected on WhatsApp is not a matter directly related to union rights, so we must reject this issue. (...)

The transmission of these DNIs through WhatsApp by the appellant's union representative does not indicate that she has acted in the legitimate exercise of her right to freedom of association. Your right to inform workers of events of union relevance does not include sending information about the ID of the workers who were part of the WhatsApp messaging group. For all of the above, the resolution of the AEPD is confirmed.

---

Also **related to the principle of confidentiality**, it is appropriate to cite the **Judgment of February 9, 2023** issued in Appeal No. 770/2020, which dismisses the appeal filed by a telephone company against the sanctioning resolution of the AEPD, in relation with the **issuance of duplicate SIM cards**.

The AEPD considers that the disputed facts violate art. 5.1.f) RGPD because the principle of data confidentiality has been affected given that the telephone company provided persons other than the owner of the mobile phone with duplicate SIM cards, which constitute the medium through which personal data is accessed. personal of the affected person. Access to the owner's personal data by a third party

occurred because the company did not have sufficient or appropriate measures in the terms of the aforementioned art.

5.1.f) of the RGPD to verify that the person requesting the duplicate SIM card is the owner of the SIM card.

The appellant alleges, among other issues, that the classification made by the Agency lacks sufficient motivation, since the facts must be subsumed in article 32 GDPR and not in article 5.1 f).

The Chamber considers the classification sufficiently motivated and confirms the Agency's criteria indicating that (...) article 32, as highlighted by the State Attorney, although related to 5.1.f), does not circumscribe the principle in its entirety, since article 5.1.f) of the RGPD requires a loss of confidentiality for its application. loss of data confidentiality, which, according to the sanctioning resolution (page 671 of the file), is accompanied by insufficient security measures. The plaintiff alleges that art 5.1.f) RGPD is limited to stating the informing principles of data protection, while article 32 includes a specific violation of security measures. However, from reading article 5.1.f) RGPD, transcribed above, it is clear that it is not limited to stating one of the basic principles for treatment (integrity and confidentiality), nor can it be considered generic and imprecise, or of insufficient determination of the sanctioned conduct, but rather allows predicting with a sufficient degree of certainty the conduct that constitutes an infraction, therefore, according to the reiterated doctrine of the Constitutional Court (...) it does not violate the principle of typicality. (...)

Lack of guilt is also alleged since the entity understands that objective responsibility is being demanded. The Chamber rejects these arguments and confirms the Agency's criteria by pointing out that Regarding the alleged objective responsibility, the appealed resolution does not consider (...) responsible for the result, but for a loss of confidentiality linked to the insufficiency of the measures. security measures implemented and, ultimately, due to a lack of diligence on the part of said entity (...) the mere verification of

The basic information of a person, such as the name, surname and ID, is useless for the purposes for which it is intended, since it is assumed that criminals who have already obtained a series of data such as access data or credentials of a person's online banking and the telephone number associated with that account, surely have the basic information of said person. It is argued that (...) she was deceived by having submitted, along with the request for a duplicate SIM card corresponding to claimant 1, a false DNI and a report of theft, and although it is true that in that case falsified documentation was provided, omits that in the case of claimant 2, the duplicate SIM was activated through the telephone channel and the recording was provided, it was verified that the operator asked the line number and the operator himself told him the name and asked if it was him, but it doesn't even ask for your ID. This last form of action also occurs in other cases of activation of duplicates by telephone channel that examines the appealed resolution.

Therefore, there has been a loss of confidentiality of the data because the security measures implemented by the data controller were not adequate or sufficient to guarantee it. This lack of diligence on the part of (...), as data controller, when implementing at source the appropriate security measures to verify that the person requesting or activating the duplicate SIM card is the owner of it is what which constitutes the element of guilt.

Another relevant aspect that is addressed in the Judgment is the consideration of personal data on the SIM card. The appellant alleges that the confidentiality of personal data is not violated since the SIM card does not identify any telephone number since said number is stored on the company's servers and the only data that said card includes is the IMSI that It is stored in encrypted form so that it is not accessible to the user, so the confidentiality of the data is not lost.

Faced with this, the Chamber reasons that following the State Attorney General's Office in its July report

As of 2016, the SIM card stores the IMSI, which is the identification code in the cellular mobile communications network and is essential to identify the subscriber, therefore, whoever has said card (the impersonator) has the IMSI stored. Furthermore, as soon as the impersonator inserts the SIM into a terminal and turns it on, the IMSI will be accessed and exchanged with the network.

To the extent that the IMSI installed on the SIM card allows an individual to be singled out and therefore identify them, it must be considered personal data, according to article 4 of the GDPR.

And it concludes by indicating that (...) both the personal data (name, surname and ID) that are processed to issue a duplicate SIM card, and the SIM card itself that unequivocally identifies the subscriber on the network, are data of a personal nature and its treatment, as well as the security and confidentiality of said data linked to the issuance/activation of a duplicate SIM card, are subject to data protection regulations. (...)

---

Regarding the **principle of legality**, the **Judgment of February 10, 2023** issued in Appeal No. 41/2021 addresses an **assumption of fraudulent contracting in the field of the energy sector**.

Therefore, the company is sanctioned by the AEPD for violating article 6.1 of the RGPD.

The resolution indicates that (...) the existence of the infringement is clearly deduced from the concise list of proven facts, which highlights that the holder of an energy distribution and supply contract with a company (ENDESA), saw how, Without their knowledge or consent, the supplying company became a different one (EDP), as well as the owner of the contract; The resolution does not consider that the data processing occurs through access to the CUPS, whose function and content we will explain later, but rather due to the lack of consent of the owner of the contract as well as the lack of adequate verification of the identity and consent of the new owner. which, in this case, acted through a representative.(...)

The Chamber clarifies that the Universal Supply Point Code (CUPS) is made up of various data, among which are in its sections c), z) and aa) personal data whose access is prohibited to marketing entities and the CNMC. , along with any that identify the owner of the supply point. Therefore, it is not access to the CUPS, which is permitted by sector regulations (Royal Decree 1435/2002, of December 27) that is sanctioned, but rather the change of ownership of the supplying company, without having the consent of the previous and the new owner, which corresponds to the new marketer or incoming marketer, in this case EDP, as set out in the contested Resolution and, in this case, such consent has not been proven, which is also evidenced by the complaint from the initial owner of the contract who, for a few days, saw his contractual relationship changed without having authorized it and without ensuring the consent of the new owner.

---

Continuing with the **principle of legality**, the **Judgment of February 14, 2023** in Appeal No. 463/2020 analyzes the **requirements of consent for data processing**.

The resolution dismisses the appeal filed by a hospital that is sanctioned by the AEPD, for obtaining the consent of the data owners without complying with the requirements imposed by the RGPD.

The facts are that in 2019, a person goes to the emergency department of a private healthcare hospital and fills out a personal data collection form indicating that in accordance with Organic Law 15/1999, of Protection of Personal Data, the data will be processed for the purpose of health care and management, identifying the person responsible, and with respect to the transfer to third parties other than these, it is stated that:

"If you do not want this information to be provided to third parties, check this box (-) Likewise, and unless expressly indicated, I authorize the person responsible for the

file (...), to the use of the patient's personal data to send information about its products and services, and may revoke said consent at any time.

If you do not want to authorize sending advertising, check this box (-)".

The Chamber confirms the sanction imposed by the AEPD considering that data protection regulations currently exclude tacit consent and require that it be explicit. Only express consent will be valid, which must be granted through a clear affirmative act that evidences a free, specific, informed and unequivocal declaration of will of the owner of the personal data, in the sense that there is not the slightest doubt. that there has been manifest will on the part of said affected person.

In the case analyzed, it turns out that the aforementioned requirements are not met in the request form for Urgent Admission to the Hospital, in that said consent is required from the patient, both to transfer their data to third parties and to send advertising, not through of active conduct, but of inaction on the part of the interested party (if you do not wish...check this box), ultimately dealing with tacit consent, without the information for which such consent is required being intelligible, as to its negative sense can lead to confusion, not being understandable to the average member of the audience.

---

Also related to the **principle of legality**, the **Judgment of March 7, 2023** issued in Appeal No. 229/2021 analyzes the **data processing carried out by the State Tax Administration Agency (AEAT)**.

It is reported by the appellant that the AEAT, within the framework of a tax inspection procedure against a third party, has issued VAT and Personal Income Tax settlement agreements containing her personal data, not being interested in said actions, and therefore has produced a

transfer of personal data of the appellant in favor of the taxpayer by the AEAT.

Specifically, it indicates that in the aforementioned settlement agreements the claimant is mentioned with her name and surname, DNI, reference is made to her family ties with third parties, property and economic data are revealed when mentioning the claimant. as owner of a tobacconist's shop and administrator of a limited liability company, data that were not known in their entirety, prior to the notification of the liquidation agreements, by the taxpayer.

The position of the State Attorney was specified in that the settlement agreements respond to the competence attributed to the Tax Administration in order to the application of taxes, as well as the fulfillment of the obligation that weighs on it in terms of motivation. of tax settlements, ex article 102.2.c)

General Tax Law.

In these terms, it indicates that in the settlement agreements the AEAT questions the expense invoices coming from the entity where the appellant is administrator, as a service provider of the taxpayer and in order to substantiate the legal obligation of the Administration. In order to justify its non-deduction of the expenses that had been invoiced to it by the entity where the appellant is the administrator, it was essential to reveal the activity and operations of the rest of the tobacconist's stores of family-related people, for the purpose to justify the instrumentalization of said entity to reduce the taxation of the owners of the tobacconists and of the company itself by recording expenses that are actually personal to the administrators and family members (including the appellant).

Well, the Chamber, after indicating that articles 6.1 c) and e) of the RGPD and 8 of the LOPDGDD are applicable, recalls what is indicated in article 95.1 of the LGT, which refers to the reserved nature of the tax data held by the Tax Administration, highlighting that they can only be used for tax purposes within their functions and within the framework or scope of their powers.



Consequently, the settlement agreements, referring to the tax obligation, respond to the competence attributed to the Tax Administration in order to apply taxes and which is developed, "through the administrative procedures of management, inspection and collection." -tion and the others provided for in this title.", article 83.3 LGT.

Tax settlements that the Tax Administration has the obligation to justify "when they do not comply with the data recorded by the taxpayer or with the application or interpretation of the regulations carried out by the same, with expression of the facts and essential elements that give rise to them, as well as the fundamentals of law." (art. 102.2.c) LGT).

In fact, in order to sufficiently motivate and prove by the Tax Administration the reasons for the rejection of the aforementioned expenses, it was essential to record the personal data that were reflected in said agreements, among others, NIF, name and surname, administration. administrator of the company, etc., This made it possible to highlight those family ties and with the company, which were considered decisive, together with other data, of the lack of justification of what was invoiced by the company of which the appellant was the administrator. to the tax obligation.

Therefore, it is not that the appellant's data included in the settlement agreements in question have been transferred to a third party (tax payer), but that said data have been used by the AEAT in the exercise of its functions and the powers attributed to the Tax Administration at the service of public interests, for tax purposes, in order to substantiate, as legally required, the instrumentalization of the company of which the appellant was administrator to reduce the taxation, among other people, of the taxpayer and justify, in short, because it was not considered deductible, the amount of the expense invoices of the aforementioned company that it claimed. Therefore, the ruling of the sentence is dismissal, confirming the resolution of the AEPD.

Regarding other principles such as minimization, in relation to the principle of proportionality in the field of **video surveillance**, it is appropriate to cite the **Judgment of May 25, 2023** issued in Appeal No. 574/2022 filed against the sanctioning resolution of the AEPD by a **Community of Owners**.

The Chamber dismisses the appeal taking into account that the fact that a video surveillance system could have been installed in accordance with security regulations does not authorize recording images on public roads beyond what is ideal, adequate and proportional. , the essential thing being whether or not through them it is capable of capturing people who are on public roads, in which case such treatment must respect the principle of proportionality, essential in this matter.

The resolution reads "Through the documentation in the file (page 1) it is proven that with the repeated cameras a viewing angle of the public transit area that surrounds the urbanization is achieved, being susceptible to capturing the image of people who pass through the same.

During the judicial process, a repositioning of the cameras was provided, and despite this, it can be seen that although part of the images are hidden by a mask, in some of them the sidewalk or even the road is partially reflected. thus making it possible to capture images of passers-by or vehicles. And this despite the fact that these images were taken on January 13, 2022, the same day that the sanctioning resolution was notified - and after becoming aware of it and the readjustment made of the angle of visibility of the exterior cameras.

That is, excessive and non-proportional processing of the images captured is carried out in relation to the scope and purposes that could justify their collection, since the requested security could also be obtained by less intrusive means for the privacy of the affected people. . For all of these reasons, the infringement found in the appealed resolution is considered proven.

In relation to the rights provided for in articles 15 to 22 of the RGPD, those that deal with the so-called Right to be Forgotten must be differentiated from those that deal with the rest of the rights.

---

Starting with the latter, the **Judgment of February 3, 2023**, issued in Appeal No. 1630/2020, addresses the exercise of rights regarding **personal data of deceased persons**.

This case is especially relevant as it involves access to special categories of data, to the medical history of a deceased person by his cousin.

The Agency resolved to grant the right of access, against whose resolution the Hospital presented the appeal, which was partially upheld.

The Chamber reasons that a literal, systematic and also teleological interpretation of articles 3.1 of the LOPDGDD and article 18.3 of the Patient Autonomy Law, "leads us to consider that relatives linked to the deceased must be understood as both the spouse and the brothers and the ascendants and descendants of the first degree, but not the rest of the relatives.

This follows from a literal interpretation given that link, according to the RAE dictionary, and in the meaning that is of interest here, means union or tie of one person or thing with another, union or tie that therefore cannot be extended to any family relationship, no matter how distant, but only to the closest ones."

The interpretation of the repeated precepts must also be related to the concept of forced heirs of article 807 of the Civil Code and with the provisions of article 4 of Organic Law 1/1982, which limits the exercise of actions to protect the rights of the honor, intimacy and image, to the spouse, descendants, ascendants and siblings of the deceased. The criteria of the AEPD must also be brought into consideration.

in its previous resolution R/01546/2016, and that of the Basque Data Protection Agency in its Opinion No. D19-008.

Limitation of access to the data of the deceased person to their ascendants, descendants, spouse and brother, lastly, which is the one that to the greatest extent protects the right to the protection of personal data, a fundamental right (article 18.4 CE) that only allows the processing of said personal data when there is either the consent of the owner or another reason for the legality or legitimization of said processing, in accordance with the provisions of articles 5 and 6 of the RGPD and articles 4 to 8 of the LOPDGDD.

Reasons, which entail the estimation of the claim of the claim, insofar as it is appropriate to deny the right to access the medical history of his deceased cousin.

---

Continuing with the **right of access**, the **Judgment of February 10, 2023** in Appeal No. 22/2021 analyzes the competence of the AEPD to determine the **correct or incorrect conduct of the data controller when resolving the request**.

The plaintiff presents an appeal against the file agreed upon by the AEPD for an alleged violation of article 22 of Organic Law 7/2021, of May 25, as the General Directorate of the Civil Guard has denied access to its data contained in file FGDO-T03.

The Chamber confirms the criteria of the AEPD, indicating that the file in question is subject to the regulations on classified matters and therefore excluded from the scope of application of the data protection laws.

Below, reference is made to the most notable rulings referring to the exercise of rights regarding files containing information on police records.

In these cases, it must be highlighted that the legal debate always focuses on the analysis of the motivation for denying the suppression of records. Motivation that is analyzed at the administrative headquarters by the AEPD and that at the judicial headquarters it is the National Court that addresses its compliance with the law.

Frequent elements in these cases are the fact that the appellants highlight that either they have served their sentence, or their criminal records have been expunged, or they were arrested, but were not convicted due to the dismissal of the case, etc. In short, reasons that the appellants understand would justify the inappropriateness of their personal data continuing to be processed in systems related to police records.

Likewise, in these cases the application of Organic Law 15/1999, of December 13, on the Protection of Personal Data, is addressed, by application of the fourth transitional provision of the LOPDGDD, for those cases prior to the application of the Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and execution of criminal sanctions.

---

The **Judgment of April 26, 2023**, issued in Appeal No. 1805/2021, analyzes the legality of the AEPD resolution that **rejects the rights protection procedure filed by the appellant.**

The facts are that the claimant sees his request for deletion of police records from the file of the General Directorate of Police (DGP) rejected, alleging that he is of Algerian nationality and is married to a Spanish citizen, who has a card. of permanent residence of a family member of an EU citizen. That the appellant's arrest occurred on April 6, 1997, that is, more than twenty-four years ago, and, since that date, the actor's reintegration has been complete. Add that it has been fulfilled

the conviction and that the criminal record has been cancelled.

The Judgment recalls the provisions of article 23 of the LOPD of 1999 (applicable at the time of the request) regarding the possibility of denying cancellation "based on the dangers that could arise for the defense of the State or public safety, the protection of the rights and freedoms of third parties or the needs of the investigations being carried out."

To then analyze the response to the denial made by the DGP to the AEPD and which focuses on the arrest of the appellant as the alleged perpetrator of crimes of membership in an armed gang, document falsification and illicit possession of weapons, the search and arrest order issued by the Central Investigative Court, as well as the prohibition of leaving the national territory for collaboration by an armed gang and finally that he was sentenced to 14 years in prison.

The DGP concludes that: "In addition, as the National Court has recalled in a ruling of September 15, 2016, the cancellation of police data is subject to a special legal regime, regardless of whether an acquittal has already been reached. that, from the perspective of data protection, the public security reasons invoked are justified, and that they support the denial of the cancellation of the requested police records"

Taking into account the above, the Chamber agrees that the denial of deletion is in accordance with the law, regardless of whether the criminal record has been cancelled, "given the seriousness and nature of the facts (...) they are effectively justified and subsisting of art. 23.1 of the LOPD, the reasons for the needs of the investigations being carried out, the prevention or repression of criminal infractions, motivatedly invoked by the General Directorate of the Police, which cover, in this specific case, the denial of the cancellation of the requested police records."

---

The **Judgment of May 31, 2023**, issued in Appeal No. 1/2022, also addresses the **deletion of data referring to police records**. The DGP denies the deletion of records requested by the appellant, because it is related to a conviction as the perpetrator of a crime of **child pornography** and because, currently, he is registered in the Central Registry of Sexual Offenders and Trafficking. of Human Beings, regulated by Royal Decree 1110/2015, of December 11.

Regarding this last aspect, the Chamber takes into account that the appellant also requested the cancellation of the aforementioned registration and it was denied on June 18, 2020 and confirmed by a Judgment of January 13, 2021. This circumstance must also be assessed. in the present case.

The Chamber rejects the appeal indicating that (...) The previous circumstance must be put in relation to the other data mentioned in the administrative Resolution, such as the nature of the stored data, the date of the sentence and the condemnatory meaning of its ruling for a crime of corruption of minors, as well as the date of the definitive remission of the sentence, immediately prior to the cancellation request, all of which justifies the denial of the cancellation or deletion of the data in response to prevention and investigation of criminal offenses and the defense of the rights and interests of third parties, in this case minors, victims of this type of crimes, so the assessment that the denial is necessary and proportionate in this case is in accordance with the provisions of article 23.1 of the General Regulation and it is therefore necessary to confirm it as it is sufficiently motivated and this motivation is in accordance with the aforementioned standards (...)

---

Regarding similar facts, the **Judgment of June 5, 2023** issued in Appeal No. 1789/2021.

The appellant was **denied deletion from the PERSONS file** because he was registered in the

### **Central Registry of Sexual Offenders and Human**

**Trafficking.** The Court highlights the nature of the PERSONS file by indicating that This police-administrative record regarding someone who has been convicted of a crime of corruption of minors contains very relevant information for the purposes of prevention and investigation of this type of crimes. and as stated by the Police DG, this file is necessary for procedures, investigations and prevention of these crimes and even when the criminal record has been cancelled, it is important to maintain this data in the police record, with the subsequent purpose of the file being the basis. for a fight against this crime that facilitates police investigations.

The Judgment rejects the appellant's claims by considering the motivation offered by the DGP and thus appreciated by the AEPD in accordance with the law, endorsing the reasons offered by concluding that: the data whose cancellation is requested, which appear in the PERSONS file, have their origin in an arrest and a criminal conviction for corruption of minors. And the maintenance of these personal data in the PERSONS file responds to reasons of public security, the need for prevention and investigation of these crimes, which makes it essential that such data be maintained in the police file.

---

This group of resolutions closes the **Judgments of June 9 and October 25, 2023**, appeals 559/2021 and 61/2022 respectively. In the latter, the **maintenance of police records despite the provisional dismissal of the case** is addressed as an element of analysis.

related to said background.

Continuing with the resolutions related to the exercise of rights, the next block addresses those sentences related to the so-called right of deletion referring to Internet search results, also called the right to be forgotten, the regulation of which is mainly found in article 17 of the RGPD and article 93 of the LOPDGDD.

The **Judgment of February 3, 2023** issued in Appeal No. 2563/2019 **rejects the claims of the appellant and confirms the resolution of the AEPD.**

The facts are that the affected person in 2018 exercises the right of deletion against Google for the result that is shown when performing a search by his name and surname referring to a link to a press release that appeared on October 6, 2016 in a Mexican media, specifically in the newspaper Proceso.

com.mx, which is titled "Money laundering emerges in Puebla de Moreno Valle" and which refers to the affected person as one of the two main shareholders of one of the (at least) 12 companies linked to a money laundering scheme resulting from drug trafficking, according to investigations by the Mexican Attorney General's Office (PGR) and the Ministry of Finance.

The appellant maintains that the right to be forgotten due to inaccuracy of the data should prevail over the right to information.

The Chamber after recalling the doctrine of the right to be forgotten in SSTC 58/2018 of June 4, and 89/2022 of September 13 referring to and SSTC 23/2010, of April 27, and 9/2007, of January, invoking article 18.1 and 4 of the Constitution and the rights of freedom of expression and information enshrined in article 20 of the Constitution, all in relation to the general interest (SSTC 107/1988, of June 8, 20/2002, of January 28, 151/2004, of September 20, and 9/2007, of January 15) takes into account that we are dealing with a news item published on October 6, 2016, and that it refers to some investigative actions (apparently of great complexity) initiated by the Mexican Attorney General's Office and the Ministry of Finance, in 2015, so the information cannot be considered obsolete, given the time that has elapsed since the issuance of the news and the facts to which it refers, which also, and because it refers to the money supposedly coming from drug trafficking, acquires great public relevance in a country like Mexico, which does not allow obsolescence to be appreciated. Public relevance that is confirmed when referring to the professional and not the personal life of the appellant.

And secondly, it indicates that "despite the plaintiff's attempts to deny the accuracy and veracity of the published information, attaching for this purpose both the certificate of lack of criminal record in his country of origin (Mexico) and data on constitution and ownership of the company Blueicon Technology SA, the truth is that the news does not even mention that said actor has been convicted, but rather the initiation of investigation proceedings against him, not only his participation in the aforementioned company, but the constitution, together with his partner, of 47 companies, in which they are registered as shareholders and/or legal representatives, sharing management positions in 12 of them. This is therefore clearly insufficient documentation and lacking evidentiary effects in order to counteract the accusation. veracity of the published news."

---

The **Judgment of March 7, 2023** in Appeal 1984/2021 **dismisses the appeal filed by the appellant against the resolution of inadmissibility** issued by the AEPD. What is relevant in this case is the ambiguous and generic nature of the deletion request.

The inadmissibility of the AEPD was based on the fact that the claimant exercised his right against the search engine in relation to a high number of links (287), deducing from this that it could be a claim contrary to data protection regulations when trying to make use of it with the sole intention of indiscriminately rewriting past events; He also based his decision on the fact that the information in the disputed URLs transcends the personal sphere as it is placed in a professional context that has not been proven to be inaccurate or obsolete, therefore, the right to freedom of expression and freedom of expression prevails. of information regulated in article 20 of the Spanish Constitution; The appeal for reconsideration against this resolution was dismissed.

The Chamber confirms the appealed resolution taking into account several factors, among which stands out that the plaintiff requested the deletion of a high number of urls (287, according to the resolution

of the Agency) who associated their name with a certain company, without specifying data as relevant as whether it was accessing media pages publishing information, opinion forums or social networks or other types of links; Furthermore, at no time did it specify the nature of the information available through the links. The generic claim that any information that associated your name with that of a certain company be dexindexed could not be upheld since it may simply be neutral information about the existence of litigation or discrepancies with certain people, in which it was mentioned. the company, which would prevent such information or opinions from being considered accurate or not, against or in favor of the claimant; In other words, the lack of data on the type of links and the content of the information fails to comply with the obligations incumbent on it (points 67, 68 and 72-74 of the CJEU ruling of December 8, 2022 cited) and prevents assessing the origin of your request and, consequently, correctly carrying out the weighing judgment on the rights at stake.

And it ends by indicating that "This conclusion cannot be effectively opposed by the fact that the search engine "Bing" has agreed to suppress access to the URLs it requested since there are 12 links, compared to the 287 in this case and it is not specified. "if on that occasion it duly justified the nature of the links and the content of the information."

---

Another Judgment that refers to the **right of deletion and the right to opposition**, but no longer in relation to internet search engines, but in the context of the internet (**in the digital medium of a journalistic publisher**) is the **Judgment of March 16, 2023**, relapsed in Appeal No. 1549/2020.

The Court maintains that we are dealing with news published on the basis of freedom of information, inserting a video that appears on social networks, which is also a means or

channel for obtaining public information. The news refers to some events that occurred on public roads, filmed by a person who captured the images, events in which the appellant was the protagonist. The news, therefore, is true news; Since it is recorded in images, it demonstrates exactly what happened, so it is not inaccurate; and its publication in the media is protected by art. 20.1.d CE. (...) we find ourselves with mere news, that news does not contain personal references of the appellant, it does not refer, at any time, to his personal life, it refers only to a public event carried out by the actor with sufficient intensity and theatricality to make known what has happened with his unfortunate behavior.

This news does not even contain an opinion or value judgment regarding the facts, it is limited to narrating such facts and their consequences. Within this narrative of events, the video recorded by a third party is very relevant, providing reality to the events since no manipulation of any kind has been demonstrated. And what is very important, this publication has not had harmful consequences either for the appellant or for third parties, so its publication is merely informative, it is nothing more than a mere publication of a news story that has occurred on the street, that seems to bother or upset the appellant but that, at the time of its recording, as stated in the aforementioned news item, he showed a happy acceptance of that recording. It is news published on April 24, 2017 but it cannot be considered obsolete, although some time has passed since the events occurred and the news was published, the truth is that they have public relevance, it is still public news, a information that is not obsolete (as required by article 17.3 GDPR). And with regard to the right of opposition, the assumptions of article 21 RGPD have not justified the concurrence of anyone to exercise said right."

For all these reasons, the appeal is dismissed and the resolution of the AEPD is confirmed.

Regarding the jurisprudence of the **Supreme Court**, the **Judgment of November 22, 2023** number 1520/2023 that **resolves the Cassation appeal 5352/2022 stands out.**

The question of cassational interest is specific to determining whether the actions of the State Tax Administration Agency (AEAT) violate article 8 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of rights. digital with the inclusion of any personal data of third parties not interested in the tax procedures, and if their treatment in said procedures is considered a transfer of personal data based on compliance with a legal obligation for the purposes of current regulations. of data protection.

The high court says that the use of personal data of third parties, other than the taxpayer, by the Tax Administration, without the required consent, must be considered legitimate, as inferred from the doctrine of the Court of Justice of the European Union set out in the sentences of September 27, 2017 (case C-73/16) and July 22, 2021 (case C-439/19), in those cases, responds to objectives of general interest related to the pursuit of tax fraud, and the processing of personal data is proven to be proportionate and does not exceed what is strictly necessary to fulfill such purpose, and occurs within the framework of a procedure in the processing of which the protection of the fundamental rights and freedoms of the interested and affected.

It also rules out the violation of article 95 of Law 58/2003, of December 17, General Tax, since the AEAT does not allow the recording of certain personal data of the appellant, referring to the identification of the name and surname,

DNI, family ties and economic data, is carried out for the effective application of taxes, as provided in article 5 of the General Law

Tax, within the framework of the powers of the State Tax Administration Agency, in the course of a procedure to verify compliance with tax obligations,

proving suitable and necessary for the effective application of tax regulations, to the extent that it was essential for the correct exercise of the collection function.

Nor does it appreciate that article 102.2 c) of the General Tax Law is violated, since the use of the personal data of the current appellant was necessary, due to the concurrent circumstances, referring to the family and professional ties existing between the employee. of the company providing professional services that issued the invoices and the taxpayer, to be able to substantiate the Settlement Agreements, and guarantee the right of defense of the taxpayer, who has the right to know precisely the list of facts that justify -can the preparation of the minutes of the liquidation proposal by the Public Treasury, which means that, in order to comply with the requirement of motivation of the tax acts, those personal data of the current appellant must appear that, as we have explained, are revealed adequate, suitable and proportionate for the fulfillment of the same purpose.

Therefore, it establishes the following doctrine of cassational interest: Article 8 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights and article 6.2 c) and e) of the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons with regard to the processing of personal data and the free circulation of these data, which provides that the processing of personal data will be lawful, among other cases, when it is necessary for compliance with a legal obligation applicable to the controller, or when it is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the controller. of the treatment, do not oppose the State Tax Administration Agency, in the course of processing and resolving a tax management, inspection or collection procedure, from using personal data of third parties, other than the obligated subject. tax subject to the administrative file, as long as the treatment

of the data is protected by the powers conferred on the tax authorities to fight against tax fraud, that the inclusion of the data is limited to those that are revealed to be adequate, suitable, relevant and necessary for the determination of the facts and motivate the resolutions that are adopted, and that they be proportionate to the legitimate purpose pursued for which they are processed.



Finally, regarding the jurisprudence of the Court of Justice of the Union European Union, during the 2023 financial year, the following Judgments deal with essential aspects of the right of access provided for in article 15 of the GDPR.

Firstly, **the STJUE of January 12, 2023**, Case C-154/21, which addresses whether the right of access includes knowing **to whom the data has been communicated**, analyzes whether specific identification is necessary. or is satisfied with reporting on the categories of assignees.

The right is requested before a postal operator, and in the judicial process it was reported that the data had been transmitted to computer companies, directory providers, advertisers that operate through mail order establishments, NGOs and political parties, among others. others. The Court establishes that the data controller is obliged to provide the interested party, upon request, with the real identity of said recipients. Only when it is not (yet) possible to identify said recipients, the controller may limit itself to indicating only the categories of recipients concerned.

try.

Secondly, **the STJUE of May 4, 2023**, Case C-487/21, clarifies that the right to obtain a “copy” of personal data implies that **an authentic and intelligible reproduction of all such data is delivered to the interested party**.

This right implies the right to obtain a copy of extracts of documents, or even entire documents, or extracts of databases, that contain said data, if this is essential to allow the interested party to effectively exercise the rights conferred by the RGPD. .

A purely general description of the data being processed or a reference to categories of personal data would not correspond to “copy”. It must be interpreted as the right to obtain an authentic reproduction of your personal data.

---

And, thirdly, and closely related to the aforementioned STJUE of January 12, it is appropriate to cite the **STJUE of June 22, 2023**, Case C-579/21, the employee and client of a financial institution is aware that others employees have consulted your data. Therefore, **it requests the identity of the people who accessed your data, the exact dates of said accesses and the purposes** for which said data was processed.

The entity refused to provide all that information because it constituted a transfer of the personal data of those people, but it did provide the dates and purposes of the accesses.

The Court indicates that, in the event of a conflict between the exercise of the rights of the interested party and the rights of third parties, a balance must be made between such rights and freedoms. And if, as a result of this consideration, it is estimated that knowledge of that information is essential to allow the interested party to exercise their rights and freedoms, said access may take place.



## 2.2 Technological

### 2.2.1 Management of notifications

#### personal data breaches

In compliance with the obligation established in article 33 of the RGPD, during 2023 the AEPD has received a total of 2,004 notifications of personal data breaches, with an increase of 10% over 2022. Of the notifications of the gap received, approximately 18% corresponds to the public sector and 82% corresponds to the private sector. In general, the breaches that affect a higher number of people are those related to ransomware-type cyber incidents and intrusions into information systems.

mation that result in exfiltration of large volumes of personal data. This type of gap affects both public and private entities.

As a result of the notifications, 30 resolutions have been issued to force the communication of the gaps to the interested parties themselves. At the same time, as a result of the initial analysis of the gaps carried out by the DIT, they have been transferred to the Subdirector General of Data Inspection on 16 occasions for a second, more exhaustive analysis.

**In total, as a result of the obligations established by Article 34 of the GDPR, approximately 17 million affected data subjects were notified by those responsible that their data had been breached.**



Within the scope of collaboration with the National Cryptological Center (CCN), the AEPD message was updated in the LUCIA tool in which entities that report a breach to the CCN are reminded of their obligations in relation to what is established in articles 32 and 33 of the RGPD in those cases in which the breach reported to the CCN affects the scope of personal data protection.

### 2.2.2 Prior consultations

3 prior queries have been received that have been resolved negatively due to not meeting the minimum requirements referred to in Instruction 1/2021, of November 2, of the Spanish Data Protection Agency, which establishes guidelines regarding of the Agency's advisory function, in accordance with the GDPR. Despite what is established in Instruction 1/2021, in general, an erroneous interpretation remains in relation to compliance and risk management, understanding that both concepts are identical.

Likewise, the erroneous interpretation persists in relation to the purpose of the prior consultation in terms of a prior validation by the Control Authority of what is indicated in the Data Protection Impact Assessment (DPIA) instead of the advice of the Control Authority in relation to those risks in which the person responsible has not been able to sufficiently mitigate as required by article 36 of the RGPD.

### 2.2.3 Help resources: guides and tools

Within the work of promoting data protection as a factor of trust and quality assurance to promote the development of the digital economy, the Innovation and Technology Division has published three guides that clarify the existing criteria regarding spaces of data, cryptographic systems and presence control treatments through biometric processing operations:

#### Approach to Data Spaces from the RGPD

#### Guidelines for the validation of cryptographic systems in data protection

#### Guide on Presence control data processing through biometric systems cos



In the line of work of evolution of the tools, the **GESTIONA-RGPD** tool has been updated adding functionality

for risk identification, mitigation measures and capacity for the management of multiple high and low risk treatments to respond to the obligations of the GDPR in terms of risk management, registration of treatment activities, treatment inventory and measures of security. Like other tools, **GESTIONA-RGPD** has been equipped with the capacity to issue reports aimed at signature by those responsible and in charge, as well as drafts related to the registration of processing activities and the processing inventory. The tool currently has the capacity to manage more than five hundred treatments from the same controller in a single file, which is why it is expected to be very useful for controllers and, especially, for Public Administrations.



To complement the Guidance guide for the validation of cryptographic systems in data protection, the

**VALIDA-CRIPTO RGPD tool has been developed and published.**

where the criteria of the guide are transferred to facilitate the management of the encryption requirements for the processing of personal data with an eminently practical approach, thus responding to the queries that are sometimes made to the AEPD in relation to the validity or not of the cryptographic systems on whose requirements it is up to the person responsible to make appropriate decisions to protect the data of the interested parties.



In relation to the obligations of articles 33 and 34 of the RGPD related to the notification and communication of data breaches, the **ASESORA-BRECHA** tools have been updated

and **COMMUNICATION-GAP** providing these tools with the capacity to issue reports that can be used as documentation to demonstrate compliance. This demand was collected by the DIT from public sector data protection delegates who stated that these reports were very useful for the management of personal data processing.



#### 2.2.4 Promotion of the development of digital economy

In relation to the new developments of the digital economy, the DIT has organized the **AEPD-ENISA International Conference on European Data Spaces** in which experts and professionals from European public administration, research and The private companies participated in conferences and round tables broadcast openly and in working groups where the synergies that can be established between the guarantees to protect the fundamental rights of people and the data access market were analyzed in a practical way. This activity represents a milestone in the activities of the DIT and the AEPD given that it is the first time that ENISA has initiated a line of collaboration in view of the interest aroused by the documents on data spaces and other matters. have been developing in recent years.

The DIT has promoted the development of projects such as the **blockchain** project to comply with the RGPD in collaboration with GMV or the Project with the Ethics Foundation on **artificial intelligence and SMEs**, a matter on which work is currently continuing.

One of the tasks that has required greater involvement from the DIT is that related to minors, especially with minors' access to content not appropriate for their age. In this aspect and with the objective of assessing the possibilities that technology currently offers, the DIT has encouraged the participation of public and private entities, giving rise to 16 meetings with public entities and 25 meetings with private entities, as well as 11 meetings with international entities. In addition to these meetings, 12 age verification tools have been evaluated to end up summarizing the conclusions of these activities in the development of 3 proofs of concept of age verification systems for the protection of minors.

Within the scope of these activities, a contract has been made with the General Council of Official Colleges of Computer Engineers of Galicia in order to reinforce the impulse that has been carried out by the DIT, on the other hand and in relation to the evaluation of age verification systems, a study contract has been made with the URJC.

Within the line of minor protection, the DIT has been active participating in the **Minor Access Group to Inappropriate Content** and in the **Minor Age Verification Group** from where it has been collaborating in the analysis of the situation and possible options that technology offers in this area.

The DIT continues to collaborate in the development of **anonymization** guidelines in the field of activities carried out jointly in the EDPB and has participated with the **SEDIA in the Data Group** through a presentation on anonymization in order to promote this requirement demanded by the article 32 of the GDPR as a guarantee of privacy.

With the objective of promoting data protection in its technological aspects to safeguard the rights and freedoms of natural persons in the field of development of the digital economy, **the DIT has developed and collaborated in the following presentations and activities:**

- ÿ Presentation at Blockchain Intelligence Law Institute
- ÿ Presentation at the BIDA Observatory presenting the Guidelines on Data Spaces
- ÿ Presentation at the Global PETs Network for Data Protection Authorities on Validation of Encryption Systems
- ÿ Presentation at the IPEN on AI topics
- ÿ Conference at the CEDPO "Confederation of European Data Protections Organizations" on AI
- ÿ APEP presentation on data breaches
- ÿ ISMS Forum encrypted presentation
- ÿ AUTELSI Observatory Podcast on AI
- ÿ Presentation at the GDPR Seminar for Korean Businesses in EU
- ÿ Presentation at the GPEN of the Guidance on encryption
- ÿ Conference at the Meeting of Authorities Proficient in AI
- ÿ Inaugural day of the Higher Course of Data Protection Galician School of Public administration
- ÿ Healthcare Cybersecurity Congress

ÿ INNOVA Sevilla S3: National Perspective in the management of Data Spaces

ÿ Association of Foundations - Demos Forum – Security

ÿ Future of Privacy Forum - Age Verification

ÿ AECOPS Zaragoza

ÿ Smart Public Procurement Congress – Valencia

ÿ Generalitat Education Ministry Congress Valencia

ÿ EU-Consent Age Verification Conference

ÿ Jurisprudence and Current Events Seminar International

## ÿ 2.2.5 Promotion of research scientific-technical

Another aspect in which the DIT develops its activities is the promotion of the development of scientific-technical research. To achieve this, we have had the collaboration of public and private entities with which the following **activities have been carried out** :

ÿ Collaboration protocol with the United Nations University in the field of Blockchain

ÿ Collaboration protocol with the Bioethics and Law Observatory of the UNESCO Chair University of Barcelona

ÿ Third and Fourth Study Space Meeting Expert AI for mutual advice on privacy/research issues

## ÿ 2.2.6 Adaptation of public administrations guides and recommendations

The DIT develops activities aimed at promoting protection in the field of public administrations. In order to respond to the challenges that have arisen in this area, articles have been developed with recommendations on the following aspects:

ÿ **Internet: Guidance for the use of cookies in the AAPP**

ÿ **Gaps: Guidance on massive gaps in the AAPP**

ÿ **EIPD: Guidelines in the Evaluation of Regulatory Impact**

In areas such as gaps and documents of a technological nature, collaboration with the Autonomous Authorities is maintained, which is already part of the daily activities of this Division.

Also in the area of Local Administrations, the DIT has collaborated in the Data Protection Day organized by the FEMP.

In relation to electoral processes, the DIT has participated in the Coordination Network for security in electoral processes.

Regarding the implications of AI, the AI sandbox has collaborated in the review of guides that will respond to the requirements that must be addressed by the AI projects that offer to participate in this sandbox.

### 2.2.7 International projection in proactive responsibility: framework European

Within the scope of the **international projection** of the DIT, the activities that have been developed can be grouped as follows:

#### EUROPEAN COMMITTEE FOR THE PROTECTION OF DATA:

- Participation in the Technology Subgroup
- Completion of the EDPB/ETicas project on AI
- Co-speakers in the "Blockchain Guide"
- Co-speakers in the "Anonymization Guide"
- Co-speakers in the "Pseudonymization Guide"
- Co-speakers in the interplay drafting team AIA-GDPR
- Participation in the Mobile Apps Expert Exchange
- Questions on SMEs & Days
- Completion of the "Coordinated action: Use of cloud based services in the public sector"

#### EUROPEAN AUTHORITIES:

- Collaboration with the CNIL on tools about data breaches
- Participation in the ChatGPT TaskForce

#### ENISA:

- ENISA Engineering Personal Data Publication Sharing (co-components)
- Participation as observers in the ENISA's Ad-Hoc Working group on Privacy Engineering

#### EU4DigitalUA:

- International Conference in Warsaw AEPD-Ukrainian Authority-Polish Authority
- MoU with the Ukrainian Authority

- Carrying out two Internship actions with a total of 7 members of the Authority Ukrainian
- Development of an online tools workshop
- Development of three activities: AA.PP., Content Withdrawal, Artificial Intelligence

#### BLOCKCHAIN:

- European Blockchain Observers Regulatory Sandbox

#### PET's:

- Meeting with the Global PET Network of DPAs

### 2.2.8 Dissemination actions

The dissemination actions carried out by the DIT respond to the new approaches that technological developments entail in relation to privacy and the protection of the rights and freedoms of natural persons. Particularly when these technological developments are novel, or when errors of concept are shown in the queries posed to the AEPD or in the forums in which members of this Division participate.

The response to these novel approaches or these conceptual difficulties is carried out through short documents in the form of articles of a technological nature published, generally, on the [AEPD blog](#). The articles published during 2023 were the following:

1. Neurodata II
2. Review of privacy measures
3. Risk of re-identification
4. User Behavior Analysis (UEBA) and data protection

5. AI-1: System vs Treatment
6. Federated Learning: Artificial Intelligence without compromising privacy
7. Artificial Intelligence: principle of accuracy in treatments
8. Citizen Folder: Transparency of the AAPP and exercise of citizens' rights
9. Digital currencies
10. Artificial Intelligence: Transparency
11. Data spaces, sovereignty and data protection by design
12. Synthetic data and data protection
13. Artificial Intelligence System: just one algorithm or several algorithms?

Likewise, the DIT participates in the webinars developed within the fourth season of the women and science cycle, which is part of the scope of the social responsibility activities of the AEPD and in which the prestige and leadership of women in the field of science and technology and where women of recognized prestige tell in first person their vision as professionals in relation to the protection of personal data.

During this fourth season the following conferences were held :

- **Online dependency, misinformation, manipulation, harassment and surveillance**, Esther Paniagua
- **Journey to the world of privacy engineering** , Isabel Barbera
- **The future of cryptography**, Maria Isabel Gonzalez
- **Can we consider data breaches a type of cyber crisis?** Cristina del Real

## ➤ 3. At the service of citizens.


# Protecting people in a digital world

The citizen service team, in accordance with the functions attributed to the AEPD by articles 57.1.b) and e) of the RGPD and 47 of the LOPDPGDD; and Instruction 1/2021 of the AEPD, has answered in 2023 more than 50,000 individual queries from citizens, written, formulated through the electronic headquarters, by telephone and through in-person assistance.

In all the responses, the 51,544 citizens who have consulted the Agency have been informed and sensitized about their data protection rights, how to exercise them and the possibility of making complaints; and, in addition, efforts have been made to facilitate the understanding of the risks, guarantees and rights related to the data processing that affects them.

In addition to these consultative actions, an important novelty that reinforces the Agency's information promotion has been the launch, in April 2023, of a continuous (24/7) and immediate attention channel for the most common doubts and questions. This channel is offered through the Agency's website and is identified on the website with a blue balloon. The new channel is provided through a Chatbot mechanism and offers the possibility that, if help is not found in the robotic response, the query is referred to a personal operator.

The results of the Chatbot in its first year of operation have been excellent, yielding figures of 17,337 queries resolved in 7 months of operation and with a level of satisfaction reported by the users themselves of 75%. The entire knowledge base of the Chatbot has been prepared by the Agency's citizen service team and is regularly updated, adapting it to the regulatory and criteria changes that occur.



It is worth highlighting that the Agency's consultative activity has increased by 48.33% compared to the previous year, which has shown the commitment of the citizen service team.

Also, as in previous years, **the frequently asked questions have been updated** (FAQs, for its English acronym) published on the AEPD website, with the aim of bringing closer and making citizens' access to the most in-demand issues in data protection more accessible and agile.

**Regarding the matters subject to consultations, throughout 2023 the most frequent consultations have been those related to claims, followed by consultations on the application of the General Data Protection Regulation and rights.**



This year, it is worth **noting** a significant number of queries regarding **time control using biometric data** and also about **advertising calls from energy marketers**, even in cases in which citizens were on the advertising exclusion list.

Regarding the **complaints received**, the following is observed:

ÿ Inappropriate use of the complaint form, which is used to communicate opposition or disagreement with certain data processing: spam advertising, advertising harassment, defaulter files and conflictive surveillance video cameras. **These are "complaints" about the actions of other responsible parties, or third parties, but not about the functioning of the Agency.**

These so-called complaints are channeled and responded to as queries and counted as queries for statistical purposes.

ÿ Complaints have also been received **related to problems with access to the website**, and with the use of forms to file complaints, the use of which was launched this year.

ÿ In the reference period, of a total of **136 records submitted with a complaint form**, **111 have been processed as queries**, because they were not complaints, and only 25 have been processed as complaints.

## 3.1 Education and minors



The Education and Minors Area has received 4,049 queries during

2023, the details of which are included in the second part of this Report in the section The Agency in figures.

This figure represents an increase of 71% compared to the previous year.

The queries have been categorized according to who makes them, or from where, as has been done in the Reports of previous years. The channels enabled by the AEPD to consult issues related to Education and Minors are: **Electronic office**, email from [canaljuven@aepd.es](mailto:canaljuven@aepd.es), WhatsApp and telephone.

Before assessing the classification of queries, we must highlight the significant increase in **calls received** this year, a total of **2,029**, which represents an **increase of 63%** compared to the same period of the previous year.

It should be noted that not all the queries received by this means respond to the scope of the Education and Minors Area (1,005), which have not been included in the classification as they are outside their scope subject.

Taking into account the queries from the educational field and minors and dividing by the category of "who makes the query", it is worth noting that the majority of them come from parents (52%) regarding the processing of their children's data, both in their relationships with third parties (education, sports, social networks) and at the family level. In the latter, queries are mainly raised about the publication by family members of images on social networks. In principle, this dissemination could be assessed as personal or domestic (art. 2.2.c GDPR) and, therefore, outside the scope of data protection regulations, but the majority of publications are made by family members, not just parents.

Other recurring queries made by parents are those related to the processing of personal data of minors in the sports field, an issue that increasingly worries families, especially in cases of the recording and dissemination of images of children and girls while practicing sports in competitions usually organized by sports federations.

**In the educational field, the percentage of consultations made by teachers, heads of studies and directors of educational centers, CEIP and IES reaches 11% of the total.** The queries are related to the processing of personal data carried out by educational centers and, above all, general information is requested with the argument of lack of knowledge on the subject and lack of training in data protection.

Regarding the queries made by **university professionals, 2%**, the majority is focused on data processing on the occasion of online exams or final degree and master's degree projects.

Inquiries have also been received from **private companies (7%)**, usually sports clubs, children's entertainment companies or language or music academies that process personal data of minors, motivated by the need to know the personal data protection regulations, fundamentally in terms of video surveillance treatments and publication of images on their websites or social networks (RRSS).

In this specific area, queries regarding the publication of images of minors on the Internet collected in activities organized by those responsible for the companies or clubs take on special significance.



In the **Public Organizations section**, 2% ask questions about local entities.

The two most common typologies in this area are the publication of images of minors carrying out sports activities in municipal pavilions and the publication of images in social media profiles of the local entity collected during popular events or festivals.

Another section worth highlighting is the queries made by **students**, both minors and adults, in this case from university students (5%). Fundamentally, the queries are motivated by the information that educational centers and universities convey to their parents, such as information about the grades of their sons and daughters.

Finally, within this assessment of the queries received in 2023, it should be taken into account that numerous queries have been answered, 14%, made by parents or professionals who want to claim the processing of their personal data carried out by both companies and Public Administrations.

From this Unit the Agency provides precise information, since on many occasions it does not appear that the claims have a well-founded basis for their admission by the AEPD. Usually the error is caused by the still belief that, for any processing of personal data, the consent of the interested party is required.

Aside from the queries received in the Education and Minors Area, it should be noted that, from the **AEPD Priority Channel**, whose management is carried out by the General Subdirector of Data Inspection, a total of 33 complaints formulated through the specific channel for minors (14 - 17 years) have been referred to this area, but which, since they do not meet the requirements of the Priority Channel, transfer is made for processing as queries.

**29 of them have been answered** and the rest were archived, given that, among other issues, there was not enough contact information to be able to establish contact with the complainants.

In the field of **protection of minors in the digital field**, the following have been maintained during 2023:

#### 📅 Meetings

- **State School Council** on February 9 and 24.
- **Working Group on Digital Addictions and Online Access by Minors to Inappropriate Content** (currently "Minors, Digital Health and Privacy"), with representatives of different public organizations at the state level to assess and promote initiatives regarding access, by minors, to online content for adults and addictive behaviors to technology that constitute a serious risk for their development and entail serious consequences in their family, educational and social spheres, February 23.
- **Age Verification Working Group**, with representatives of different state-level public organizations (Ministry of Economic Affairs and Digital

Transformation, CNMC, FNMT and Ministry of the Interior) on the creation of an attribute for the age verification of minors (+18 years) prior to accessing inappropriate content on the Internet, (pornography, online gambling), March 24.

- **Working Group on Guidelines for Responsible Use of the Internet** with the Ministry of Education and Vocational Training, the Government Delegation for the National Plan on Drugs, INCIBE and the Councils of Official Colleges of Physicians and Psychologists, to address action measures against the use addictive or problematic that minors make of ICT, March 29.
- **Working Group Problematic or addictive use of the Internet by minors** with Councils of Official Colleges of Physicians and Psychologists, the Ministry of Education and Vocational Training, the Delegation of Government for the National Plan on Drugs, INCIBE, the General Directorate of Health Public and the State School Council, with the objective of addressing measures of action against said behaviors, search for

resources for identifying the problem and action measures for families, May 4.

- **Spanish Association of Pediatrics.** In order to promote avenues of collaboration, as well as the dissemination of materials and content to support families in relation to behavioral addictions, June 8.

#### 📌 Collaboration in training activities

- **NOOC Minors and Network Security Course**, 4th edition carried out in collaboration with INTEF and INCIBE, with the aim of publicizing guidelines, tools and strategies that allow avoiding the risks of inappropriate or unsafe use of the network, and guiding and accompanying minors in the digital environment and safeguard your personal privacy and well-being. Aimed at the entire educational community. 1,583 students enrolled.
- **MOOC course Educate in digital security and privacy**, 2nd Edition managed from the INTEF open online course educational platform in which INCIBE, INTEF and AEPD participate. In this edition, 1,372 students have enrolled, with a teaching profile.
- **Tutored Course Protection of personal data in educational centers**, 3rd Edition 3, organized by INTEF and AEPD, 150 teachers from non-university centers and education inspectors from the different Autonomous Communities participate.
- Participation AULA 23 (IFEMA), March 25, in collaboration with the State School Council, training representatives of 30 AMPAS.
- Digital Classrooms of the Coca Cola Foundation where the **Guide that does not come with the mobile phone** was presented with the 10 keys that families should have when giving their children their first mobile phone. III Family Congress in Malaga, where he will participate in a Round Table entitled "Current challenges in minors and adolescents: Harassment on social networks.

Bullying".

- Conference organized by the National Health Insurance Group, under the title Connected and Protected?, on the risks that exist in the use that minors make of mobile devices.

#### 📌 Materials published by the Area of Education and Minors

- **Basic criteria for the Processing of personal data in Educational Centers**, published in September.

#### 📌 Dissemination of materials related to minors and the internet

- Dissemination of the **"More than a mobile" campaign**: sending information and documentation about the campaign, which includes the "Guide that does not come with the mobile phone" to collaborators and contacts of the Education and Minors Area from Canal Joven, on February 12.
- Dissemination of the 2023 Good Educational Practices Awards, after the publication in the BOE of the call for the AEPD Awards, the information is disseminated to collaborators, Departments of Education of the CCs. AA, Data Protection Delegates of the CC Education Departments. AA, CEAPA, CONCAPA and Family Associations through the Youth Channel, on May 22.
- Dissemination of the **Digital Family Plan** of the Spanish Association of Pediatrics (AEP), defined as a platform with useful information on the appropriate use of the Internet by children and adolescents and aimed at families and paediatricians, is sent through the Young Channel, on 16 October. The information has been sent to the Data Protection Delegates of the Family, Education and Health Departments of the different CCs. AA, and the most representative Family Associations (CEAPA, CONCAPA...). In addition to general information, the summary infographic has been added to the communication .
- Dissemination of the **basic Criteria for the Processing of personal data in Educational Centers**, September 18.

## 3.2 Communication

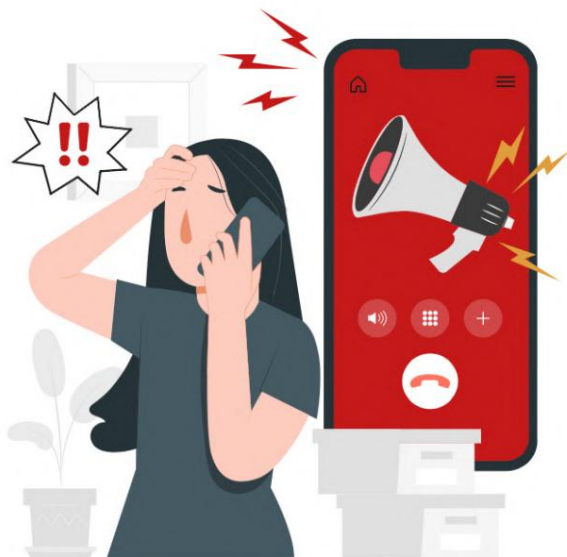
The actions carried out by the Agency in 2023 have been accompanied by their respective communication initiatives with the aim of promoting their dissemination among citizens, data controllers and data processors, and data protection delegates. Below are those related to the press and communication department, as well as the institutional agenda launched by the AEPD to promote knowledge of them.

### 3.2.1 Social networks

#### X, LinkedIn, YouTube and Instagram

In 2023, the Agency has continued to disseminate materials and advice **through its profile on the social network** (formerly Twitter), increasing new followers by almost 2,000 and with more than 800 tweets published this year. **It thus exceeded 37,600 followers**, with the most notable tweets being the following: the beginning of previous investigation actions into OpenAI, the changes to article 66.1 b) of the General Telecommunications Law and advice for families related to data protection and digital education for minors and adolescents.

## DERECHO A NO RECIBIR LLAMADAS COMERCIALES NO SOLICITADAS



In May 2022, the Agency activated its **profile on the social network LinkedIn** to expand both its online presence on social networks and the dissemination of the content and initiatives it carries out, so 2023 is the first year in which its evolution can be fully analyzed. . The topics are common to those that the Agency addresses on other social networks, but LinkedIn's own characteristics allow it to explain the issues that are disseminated in more detail, generating a direct reaction from users. The profile has increased followers by more than 7,000 in 2023, exceeding 20,000, with more than 220 posts published (which were seen by more than one million LinkedIn users - 36% more than in 2022) and more than 72,000 interactions . Thus, **there were more than 28,000 reactions, almost 300 comments were left, almost 7,000 users shared the posts on their LinkedIn profile and clicked on the links in the posts 37,000 times.**

The **most notable topics** that were published on the LinkedIn profile are the following: Start of investigation into OpenAI, the modification of the LOPDGDD, and the changes to article 66.1 b) the General Telecommunications Law.

Likewise, work has also continued on the **profile that the Agency maintains open on YouTube**. The AEPD produces multimedia content with which it aims to facilitate the understanding of some data protection concepts, as well as to disseminate the initiatives it carries out. In 2023, there have been more than 240,000 views of the channel's videos and 13 new videos have been published.

This channel includes **four types** of videos:

- the recording of conferences, talks or webinars organized by the Agency;
- videos with advice or recommendations;
- video tutorials to configure privacy options in browsers, operating systems, social networks and most popular apps,
- and the awareness campaigns carried out by the AEPD.

In aggregate, the most viewed content on the Agency's YouTube channel is related to the **configuration of privacy options for social networks and other Internet services** (Configure your privacy on Facebook, TikTok, YouTube and Whatsapp), in addition to the campaign video **'For everything behind'** (He committed suicide because everyone saw the video in which he appeared).



Regarding the most viewed videos of 2023, the **'Change the Plan' campaign stands out**, carried out together with the Spanish Association of Pediatrics, as well as the privacy configuration videos and the webinars of the 'Woman and Science' cycle, which also if broadcast live, they are also recorded and made available to users on the YouTube channel.



Regarding **Instagram**, the Agency launched its **official profile on the social network** in September 2022. to enhance both its online presence on social networks and the dissemination of the content and initiatives it carries out. 2023 is the first full year in which the Agency has a profile on this social network. During this year, more than 150 posts have been published and almost 35,000 users have seen AEPD publications, with the most viewed content being the publication of the **'Cambia el plan' spot**, which also reached @enfamiliaaep users by making a collaborative publishing.

In terms of the number of **'likes'**, the publication that was most successful was the one on the priority channel of the **'He committed suicide because everyone saw the video in which he appeared' campaign**. It's not because of the video, it's because of everything behind it.'



### 3.2.2 Other dissemination actions

#### 3.2.2.1 AEPD monthly newsletter

The Agency prepares and sends a monthly newsletter whose main recipients are the entities adhering to the Digital Pact, the data protection delegates registered with the Agency and the people and/or entities that have specifically registered to receive it.

Its objective is to group together the launches and news of the Agency aimed fundamentally at data controllers, although it also includes some topics focused on the citizen, as well as matters that, without being new, are considered useful.

**The newsletter is also published on the web**, which allows it to be consulted retroactively and on demand. It is also sent to all Agency staff, so that all AEPD workers know the news about the initiatives launched.

### • 3.2.2.2 The Agency's blog

The objective of **the Agency blog** is to serve as a speaker for the dissemination of different initiatives launched, as well as reports, guides, infographics or documents, among other matters, providing a close vision of both the work carried out in the organization and the data protection in a global plan.



During 2023, the Agency's Blog has received more than 650,000 unique visits .

Among the posts that have aroused the greatest interest are those related to:

- ÿ Dissemination of videos with violent content on social networks
- ÿ Anonymization and pseudonymization
- ÿ Use of biometric data
- ÿ Personal data security breaches: what they are and how to act
- ÿ When to review data protection measures
- ÿ Can schools take images of students during their school activity? And upload them to the internet?

### • 3.2.2.3 Space "We protect your privacy"

The 'We protect your privacy' space of the **Spanish Data Protection Agency and Radio 5** offers citizens recommendations to know their rights and how to exercise them, as well as advice to facilitate compliance with regulations for organizations that process data. It premieres every Wednesday and is rebroadcast throughout the week, and all broadcast programs can be heard at any time on the **Radio website**. 5.

The broadcast began on July 4, 2018 and since then 201 thematic pieces have been broadcast, 30 of them in 2023.

### • 3.2.2.4 Relations with the media

The dissemination of data protection by the media is essential both to raise citizens' awareness of their rights and to disseminate the obligations and how to comply with the requirements established in the regulations. Throughout 2023, **the Agency responded to more than 500 media queries related to this fundamental right**. This work of personalized attention to the media was complemented by the proactive sending of press releases to the media and to the communication departments of the organizations adhering to the Digital Pact.

Likewise, **these notes are published on the Agency's main page, having received almost 700,000 visits**.

The **six most consulted press releases** in 2023 have been the following:

- ÿ **Modification of the Organic Law on the Protection of Personal Data and guarantee of digital rights**
- ÿ **The AEPD publishes the Circular on the right of users not to receive unsolicited commercial calls**
- ÿ **The AEPD received the highest number of complaints in its history in 2022**
- ÿ **The AEPD publishes a guide on data protection and labor relations**
- ÿ **The AEPD updates its Guide on the use of cookies to adapt it to the new CEPD guidelines**
- ÿ **The AEPD initiates ex officio investigation actions against OpenAI, owner of ChatGPT**

Likewise, in relation to information agenda notes published on the website, in 2023 the Agency published more than 130 meetings or public events in which different members of this institution participated. This communication activity was complemented by the Agency's participation in the press releases of the plenary meetings periodically organized by the European Data Protection Committee (EDPC).

### 3.3 Institutional agenda

During 2023, the Agency continued with its mission of promoting the culture of data protection among citizens and organizations, as well as contributing to the constant analysis of the implications of the regulations of this fundamental right in the activity of different sectors, through its virtual or in-person participation in numerous meetings, conferences, forums, conferences, courses, webinars, events and presentations, as an organizing or guest entity.



The complete list of the institutional agenda of the AEPD can be consulted in this web section.

Within the scope of the public sector, the AEPD participated in various forums, congresses, courses, seminars, meetings, conferences or workshops, such as the specialized course for Data Protection Delegates of Public Administrations; the II Conference of data protection delegates of the Rey Juan Carlos University; the II Aragonese Conference on Data Protection, Transparency and Cybersecurity, organized by the Aragonese Association of Data Protection Delegates; the III Anti-racist Week, organized by the Ministry of Equality; the course on Sustainability and Technology at the Carlos III University of Madrid; the IV Data Protection Conference of the Madrid City Council; the Course 'Digital Rights and artificial intelligence: beyond ChatGPT', from the University of Málaga or the seminar 'Challenges for data protection at the current time', from the Menéndez Pelayo International University (UIMP) of Santander.

Likewise, he participated in the meeting on 'Value-based digital health: towards the human factor and precision medicine', organized by the Ministry of Health of the Government of Cantabria and the TERA Cluster; the course 'New Technological Challenges in the Protection of Personal Data. Special Reference to the Preparation of Profiles, Big Data and Artificial Intelligence', from the International University of Andalusia; the 11th Conference on

Data Protection in Security Forces and Bodies, organized by the Europol Data Protection Expert Network (EDEN) in cooperation with the Ministry of the Interior, National Police and Civil Guard; the course 'Administration of justice and the fundamental right to data protection' from the Center for Legal Studies; the I Congress on data protection in the educational community, organized by the Data Protection Delegation of the Generalitat Valenciana and the I Conference 'The Digital Dimension of Violence against Women', organized by the Subdelegation of the Government of Segovia.

Other meetings in which the Agency also participated were the I International Congress of Clear Communication of the Rey Juan Carlos, Católica de Murcia and Autonomous universities of Barcelona; the I Cycle of dialogues 'Horizonte Iberoamérica Digital', organized by the Ibero-American General Secretariat; the I Digital Week of the Ministry of Industry, Commerce and Tourism; the INTEF 'Educate in digital security and privacy' course; the certification workshop for data processing operations and as a tool for international transfers, organized by the National Data Protection Commission of Portugal under the impulse of the EDPB Regulatory Compliance Subgroup coordinated by the Agency; the meeting on Artificial Intelligence organized by the Íntegra Foundation Chair on Identity and Digital Rights and by the Microsoft-Universitat de Valencia Chair on Privacy and Digital Transformation, and the Conference on gender violence organized by the Ministry of Justice.

On the other hand, within the framework of its Instruction 1/2021, the Agency held a meeting with Data Protection Delegates of local entities (Provincial Councils, Island Councils and Councils, provincial capitals and cities with more than 10,000 inhabitants), with the purpose of reviewing the situation in which they perform their functions, and exchanging opinions. He also did so with representatives of the DPD Association of Parliaments, with the aim of learning about its objectives as a recently created association and contributing to the development of good practices.

The search for **collaborative spaces for the protection of minors in the online sphere** was a priority and a constant during 2023, which resulted in numerous meetings with different entities, such as the State School Council and the organizations representing parents of the students (CEAPA and CONCAPA); Eurochild; the Spanish Association of Pediatrics (AEP); the FAD Juventud Foundation and the European Association for the Digital Transition or the National Markets and Competition Commission, and in attending events such as the presentation of the AEP's Digital Family Plan.

This objective was also reflected in the holding of meetings with different public officials, aimed at addressing the promotion of measures for the protection of minors in the digital world within the framework of the State Pact **'Protecting children and adolescents in the environment. digital'**, such as those held with the mayor of Santander, Gema Igual Ortiz; the Minister of Education, FP and Universities of Cantabria, Sergio Silva, the president of the School Council of the Community of Madrid, Pilar Ponce Velasco, as well as the general director of the Association of Information Magazines (ARI), Yolanda Ausin.

In addition, the director of the AEPD held a meeting with the prosecutor of the Coordinating Chamber for Minors in the State Attorney General's Office, Eduardo Esteban, and the vice president of the European Association for the Digital Transition (AETD), Ana Caballero, on the occasion of World Children's Day, in which the practical experience of the AEPD and the different actions carried out to raise awareness among families of the impact that premature and uncontrolled use of the Internet and social networks can have on minors were presented. , the most frequent crimes suffered by minors in the digital sphere and the news regarding the proposal of the State Pact for the protection of minors on the internet and social networks.

The AEPD had meetings with representatives of the General Council of Psychology, the Council General of Official Colleges of Physicians, Ministry of Education, National Plan on Drugs

and INCIBE, to address the serious consequences of the problematic use of ICT by minors and the establishment of prevention initiatives, early detection methods, based on scientific evidence, and offer guidelines for families and educational centers.

In March 2023, within the framework of the Minors Working Group established for the protection of minors in the digital sphere, the AEPD convened a new meeting, from which work began on two lines of action: one dedicated to the risks of the problematic or addictive use of digital technologies and their consequences and how to prevent, detect and address these situations, while the second focused its efforts on working on age verification to prevent access online of minors to adult content, particularly pornography.

Consequently, the Working Group adapted to these objectives, establishing itself in accordance with each of the purposes. A Technical Group was formed, composed of representatives of the Agency, the Ministries of the Interior, Economic Affairs and Digital Transformation, and Defense, General Directorate of Police, CNMC, FNMT and SGAD, in charge of age verification systems, in April 2023, which was followed by various technical meetings.

This intense work materialized, before the end of the year, with the adoption by the AEPD of a proposal for a system of age verification and protection of minors on the Internet when accessing content for adults, which contemplates, among others materials, a **Decalogue of principles** that age verification systems would have to comply to be effective and respectful of the rights and freedoms of people, in particular with the right to protection of personal data and privacy, as well as a **technical note** with project details and **three practical videos** that demonstrate how the system works on different devices, with different operating systems and using various identity providers.

The proposal for an age verification system, the Decalogue and the rest of the materials **were presented publicly on December 14** on the occasion of the 30th Anniversary of the Agency, by the director of the AEPD, Mar España, the advisor of the National Commission of Markets and Competition (CNMC), Pilar Sánchez Núñez, and the president-director of the National Currency and Stamp Factory (FNMT), Isabel Valdecabres.

This presentation would mark the beginning of a round of meetings with large internet companies such as Google, Meta or TikTok, to convey the proposal to them and demonstrate that it is technically possible to protect minors from access to inappropriate content while guaranteeing the anonymity of adults when browsing

Internet.

On the other hand, within the framework of institutional cooperation relations between authorities, the AEPD attended a meeting in Barcelona organized by the Catalan Data Protection Authority, in which the Basque Data Protection Agency (AVPD) also participated. ) and the Transparency and Data Protection Council of Andalusia. The Agency also held a meeting with representatives of the AVPD, both within the framework of institutional cooperation relations between authorities.

Finally, the AEPD continued to promote initiatives to promote the **Digital Pact for the Protection of People**, such as the meetings held with the Information Media Association (AMI) and the District Attorney coordinator of the Minors Unit, Eduardo Esteban Rincón; with the Mapfre Foundation, as well as with representatives of ASISA for the latter to sign its adhesion to the aforementioned Digital Pact.

In the private sphere, the AEPD participated in the 'Privacy Day' seminar of the Association of National Experts in Technological Lawyering (ENATIC); the Arts and Humanities Forum of the Círculo de Bellas Artes; the XX Health Data Security and Protection Forum, organized by the Spanish Health Informatics Society (SEIS); the XV ISMS Forum Privacy Forum; the table 'Minors, technology and future society', organized by the Civil Rights Section of the Ateneo de Madrid; the III Human Rights Course in the National Police; the II Congress on the Right to Personal Autonomy 'Technology in the daily lives of older people', organized by the Democratic Union of Pensioners and Retirees and the Telefónica Foundation; the Coca-Cola Foundation's Digital Classrooms program; the Conference on Data Protection and Health Research or the IX International Privacy Congress of the Spanish Professional Privacy Association.

In addition, he participated in the III Family Congress in Malaga; the 41st Symposium of the Spanish Association of Industrial Pharmacists (AEFI); the ENATIC Privacy 2023 webinar; the II Conference on Security and Privacy: Rights and obligations of the Security Forces and Corps in matters of data protection, organized by ECIJA and the International Police Association (IPA)

Madrid; an information session with students from the Stetson University College of Law in Florida; the session 'New framework for making international transfers to the United States', organized by the Foundation for Research on Law and Business (FIDE); the conference on 'Early prevention of gender cyber violence in young people', organized by the Diagrama Foundation and the IV edition of the Connected Citizenship Conference, organized by Screens Amigas.

The 'Generation XXX' work session. For effective control of minors' access to pornography', organized by the Dale a Vuelta Association; the 'Innovation and Government Managers in Private Health' Forum, organized by Pfizer; the conference 'Connected and protected?' from the National Health Insurance group; the International Information Security Day



**Digital Pact  
for the Protection  
of People**



ISMS Forum; the III Conference 'Against Abuse, Zero Tolerance' of the Mutua Madrileña Foundation and Atresmedia; the Trends 2023 event, organized by the newspaper El País and the inauguration ceremony of the new Childhood and Adolescence Section of the Illustrious Bar Association of Madrid (ICAM) were other events in which the Agency also participated.

The AEPD also held meetings with representatives of the telecommunications operators; from the Pro-Bono Spain foundation; of the Spanish Association of Family Lawyers (AEFA); of the Spanish Banking Association; from Secuware; from Women4Cyber Spain (W4C Spain); from UPS and UNO (logistics and transportation employer); from UNESPA; with a representation of the sectors related to advertising activity, as well as Google, Meta and Orange.

Within this framework, the Agency also met with representatives of foundations and associations, such as the Computer and Communications Industry Association (CCIA); the European Association for Digital Transition; the Canal Senior Association and the Association

EMANCIPATIC.

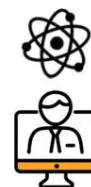
On the other hand, the Agency explored the implications of scientific advances around neurodata for the protection of personal data, through a meeting with neurobiologist Rafael Yuste.

The Agency continued to organize its 'Study Space on Artificial Intelligence', a periodic debate meeting that brings together a multidisciplinary group of experts in the field with the aim of fostering an environment of dialogue where ideas can be addressed about the current challenges that arise in the framework of Artificial Intelligence (AI), as well as new challenges, perspectives, developments, concerns and possible initiatives, to facilitate the development of an AI that respects ethical and data protection principles. In 2023 it held its third and fourth meeting. To these events we must add the celebration of "DATA SPACES IN EU: Synergies between data protection and data spaces, EU challenges and experiences of Spain", organized by the AEPD and the European Union Agency for Cybersecurity (ENISA),

with the aim of addressing the European Data Space Initiatives from a privacy perspective.

Likewise, the Agency organized conferences on different subjects, such as the 'Seniors in the digital environment' Meeting, organized jointly with the Platform for Seniors and Pensioners (PMP); a day of normative quality in data protection; the Cycle of Virtual Forums on 'Challenges for data protection in the face of technological advances', organized together with the Spanish Agency for International Development Cooperation (AECID); and moderated the webinar organized by the Spanish Agency for International Development Cooperation (AECID) on digitalization and minors, in which representatives from UNICEF Spain, INTEF, the Ministry of Education and Vocational Training, and the European Association also participated. for the Digital Transition.

In 2023, the Agency organized a new cycle of webinars on 'Innovation and Data Protection. Women and Science', with four digital debate sessions to analyze various aspects related to science and technology.



Likewise, it is worth highlighting the signing of General Action Protocols with the Platform for Seniors and Pensioners (PMP), the International Institute of Technology and Digital Law Foundation and the General Council of Official Medical Colleges, respectively, to establish a framework of cooperation and collaboration for the benefit of the rights and freedoms of people in the processing of their personal data. Within this framework, the Agency also signed a General Action Protocol with the General Council of Official Colleges of Psychologists aimed at increasing the effectiveness of care measures for people affected by digital violence, especially women, minors and members of groups. vulnerable, when their data has been obtained and disseminated illegitimately over the Internet.

At the international level, the Agency continued to participate in the plenary meetings and subgroups of the European Data Protection Board (EDPB), and held meetings with other regulators at international level, such as the virtual meeting with the Data Protection Authority of the Kingdom of the Netherlands (the ICO, for its acronym in English) or the XIII Iberian Meeting of Data Protection Authorities, held between the Data Protection Authorities of Spain and Portugal.

Within the framework of the Ibero-American Network for the Protection of Personal Data (RIPD), the AEPD participated in the XX Meeting of the RIPD held in Santa Cruz de la Sierra (Bolivia); in the commemorative meeting of the 20th anniversary of this Network, held in La Antigua (Guatemala), as well as in the online information session on ChatGPT held within the framework of the common action coordinated by the RIPD.

Within the chapter of international meetings in the field of data protection and privacy, the Agency attended and participated in the 45th Global Privacy Assembly, held in Bermuda; the Privacy Symposium, held in Venice, or the Spring Conference, organized by the Hungarian Data Protection Authority and held in Budapest.

Within this context, the AEPD received a delegation from the Ukrainian Ombudsman, who visited the Agency to carry out an internship within the framework of the project 'Reinforcement of EU4DigitalUA: institutional strengthening, communication and data protection', financed by the European Union and managed by the International and Ibero-American Foundation for Administration and Public Policies (FIIAPP). This visit is joined by the one received by a delegation from the Agency for Electronic Government and Information and Communication Technologies of Bolivia (AGETIC), to learn about the regulatory framework on data protection, the functions of the Agency as the authority in charge of ensuring for compliance with said regulations, as well as the tools and guides developed by the Agency to facilitate compliance.

It should also be noted that the AEPD and the European Data Protection Supervisor (EDPS) signed a Memorandum of Understanding (MOU) with the aim of promoting cooperation between both authorities to disseminate the right to data protection and provide a framework for the exchange of technical knowledge and best practices.

Finally, the Advisory Council of the Data Protection Agency - a collegiate advisory body to the Agency's management - held meetings on July 11 and December 11, 2023 to present and analyze the activity of the institution.

### 3.4 Infographics

In 2023, the AEPD published several infographics to complement the information provided through its channels. All of them are available in a specific section of the Agency's website and, although several of them address topics that have already been covered in formats such as guides or other more extensive documents, the Agency considers that this type of information can help both citizens and those responsible to address different matters related to data protection in a simplified way.

In 2023, the following **infographics** have been published or updated :

#### Responsibility of minors (and their parents) for acts committed on the Internet



## 👉 Recommendations for Plan families Family Digital

### 👉 How screens affect health

### 👉 Criteria for the processing of personal data in educational centers

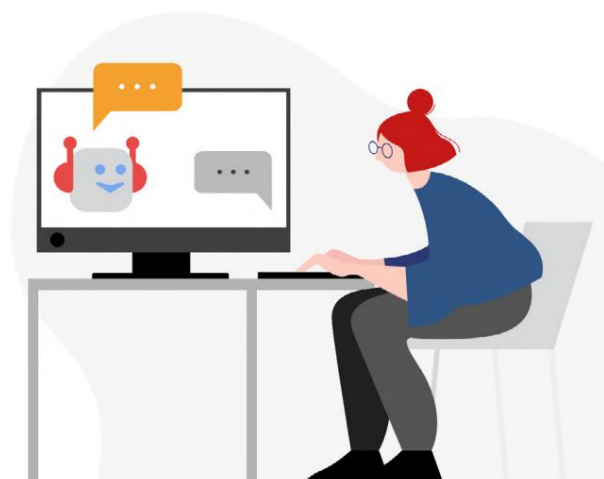
### 👉 Basic tips for families about The guide that does not come with the mobile

## 1 Planifica la llegada del móvil

Al entregar un móvil a nuestros hijos, les damos la posibilidad de acceder a una gran variedad de información, relaciones y contenidos. Pero también existen riesgos que deben conocer. Antes de dárselo, valora su grado de madurez y explícaselos.



### 👉 Recommendations for users when using chatbots with Artificial Intelligence



### 👉 Right not to receive commercial calls requested

## 👉 3.5 Presentations

In 2023, the AEPD continued its commitment to promoting a culture of data protection among citizens and organizations through different dissemination actions.

Below are the presentations organized by the Agency or in collaboration with other entities that were attended by the media:

### 👉 Presentation of the Agency's age verification criteria for accessing web pages with content inappropriate for minors and celebration of the Agency's 30th anniversary (December 14)

The director of the Spanish Data Protection Agency (AEPD), Mar España; the acting president of the Regulatory Supervision Chamber of the National Markets and Competition Commission (CNMC), Pilar Sánchez; and the president-director of the National Mint and Stamp Factory (FNMT), Isabel Valldecabres, held a meeting with the press in which the age verification criteria developed by the Agency and the next steps to be taken were presented. to prevent access by minors to inappropriate content on the Internet. At the meeting, the Agency presented a practical and effective proposal for an age verification system and protection of minors on the Internet when accessing adult content.

With the presentation of this system - composed of a **Decalogue that includes the principles that an age verification system must comply with, a technical note with the details of the project and three practical videos on how the system works on different devices-** It was demonstrated that it is technically possible to protect minors from access to inappropriate content while guaranteeing the anonymity of adults when browsing the Internet. After the press conference, the event to celebrate the 30th anniversary of the creation of the AEPD took place.



The event began with a speech by the director of the Agency in which she reviewed the 30 years of experience of the AEPD, after which the president of the European Data Protection Committee (CEPD), Anu Talus, gave a presentation where he shared the experience of the European Committee. Next, a round table was held dedicated to the 'State Pact for the protection of children and adolescents in the digital environment and the impact of electronic devices on the health and privacy of minors', in which the vice president of the European Association for the Digital Transition, Ana Caballero; the prosecutor of the Minors Unit (State Attorney General's Office), Rosa María Henar Hernando García; the Computer Crime Prosecutor, Patricia Rodríguez Lastras; the director of the National Institute of Educational Technologies and Teacher Training (INTEF), Julio Albalad Gimeno; and the president of the Spanish Association of Pediatrics, Luis Carlos Blesa Baviera.

Subsequently, the table aimed at analyzing the 'Criteria for the protection of minors in access to adult content' began, which included the participation of the director of the Technological Innovation Division of the AEPD, Luis de Salvador Carrasco; the president of the General Council of Computer Engineering Colleges, Fernando Suarez Lorenzo; the director of Telecommunications and the Audiovisual sector of the CNMC, Alejandra de Iturriaga Gandini; the commissioner and DPD of the General Directorate of the Police, Félix Jodra Abuelo; the deputy general director of Organization of Audiovisual Communication Services (SETELECO), Cristina Morales Puerta, and the director of Digital Services and Innovation of the FNMT, Raquel Poncela González.

Finally, the Attorney General of the State, Álvaro García Ortiz, and the Minister of the Presidency, Justice and Relations with the Cortes, Félix Bolaños García, were in charge of closing the event.

📌 **Call from the Spanish Agency for Data Protection, Attorney General's Office State - Juvenile Chamber - and the Association European Union for the Digital Transition on the occasion of World Children's Day (November 20)**

The director of the Agency; the Coordinating Court Prosecutor for Minors in the State Attorney General's Office, Eduardo Esteban, and the vice president of the European Association for the Digital Transition (AETD), Ana Caballero, held a meeting with the press on the occasion of World Youth Day. Childhood.

During it, the practical experience of the AEPD and the different actions that are being carried out to raise awareness among families of the important impact that premature and uncontrolled use of the Internet and social networks can have on minors were presented; the most frequent crimes suffered by minors in the digital sphere by the Juvenile Prosecutor's Office and the news regarding the proposed State **Pact for the protection of minors on the internet and social networks**, led by the AETD and agreed upon with Fundación ANAR, Save The Children, Dale una Vuelta, iCMedia and Unicef, and which has the institutional support of both the AEPD and the State Attorney General's Office.

## 📅 Presentation Digital Family Plan (September 14)

The Agency collaborated with the Spanish Association of Pediatrics (AEP) in the presentation of the **Digital Family Plan**, which included the participation of doctors Guillermo Martín Carballo, vice-president of Primary Care of the AEP, and María Salmerón Ruíz, coordinator of the Digital Health working group of the Health Promotion Committee of the AEP, and Mar España Martí, director of the AEPD.

The AEP Digital Plan, which has the support of the Spanish Data Protection Agency, materializes in a platform with useful information on the appropriate use of the Internet by minors for families and paediatricians. It also includes a document that families can personalize and adapt to their particular circumstances with scientific recommendations based on the age of their children and other general ones for all members. The collaboration established for the specific dissemination of the Digital Family Plan is detailed in the 'Collaboration initiatives' section of this Report.

## 📅 Menéndez International University Course Pelayo 2023 (July 5-7)

From July 5 to 7, the Agency gave the seminar '**Challenges for data protection at the current time**'. The seminar, organized by the Spanish Data Protection Agency (AEPD) and the Menéndez Pelayo International University (UIMP) within the framework of the Santander Summer Courses, is directed by the director of the AEPD, who appeared before the media. communication to publicize the main challenges faced by the AEPD and the importance of this fundamental right, among others, the processing of personal data of minors and the impact of Artificial Intelligence.

## 📅 Presentation of the State Pact to protect minors on the internet and social networks (June 22)

Six civil society entities - the European Association for the Digital Transition, Save The Children, ANAR Foundation, iCMedia, Dale Una Vuelta and Unicef - presented on June 22 at the Ateneo de Madrid a proposal for a State **Pact on protection of minors on the internet and social networks**. This proposal has the institutional support of the Spanish Data Protection Agency.

## 📅 Data Protection Awards 2022 (January 26)

On January 26, the AEPD presented the '2022 Data Protection Awards'. These awards recognize works that most promote the dissemination and knowledge of the fundamental right to data protection, as well as its practical application in different environments. The prizes awarded correspond to the categories of Communication; Proactivity and good practices in compliance with the Regulations and the LOPDGDD; Good educational practices; 'Emilio Aced' investigation; Entrepreneurship 'Ángela Ruiz Robles' and Good practices for greater protection of women against digital violence. The details of the awarded initiatives are included in a specific section later in this Report.



## ÿ Presentation event 'Codes of conduct as an instrument to promote agile dispute resolution' (January 17)

On the occasion of the approval of the modification of the **AUTOCONTROL Code of Conduct 'Data processing in advertising activity'**, which includes a way to more quickly resolve claims regarding data protection and advertising that may be raised by citizens, the Agency organized an event to present it. The event was inaugurated by the director of the AEPD, Mar España, and was attended by the general director of AUTOCONTROL, José Domingo Gómez Castallo, and the telephone operators MásMóvil, Orange, Telefónica and Vodafone, who signed their adhesion to it. .

### ÿ 3.6 Collaboration initiatives and dissemination

#### ÿ 3.6.1 Support for the Pact proposal of State "Protecting children and adolescence in the digital environment"

The AEPD supports the proposed **State Pact for the protection of minors on the internet and social networks** launched by the European Association for the Digital Transition, promoter of the initiative, Save The Children, ANAR Foundation, iCMedia, Dale la Vuelta and UNICEF.



The starting point of this initiative, the first of this magnitude in which the most representative child protection organizations participate, has been the shared concern about the

risks that children and adolescents face in these environments, when using services designed for adults, which can affect their socialization and enhance possible mental health problems, such as anxiety and depression, in addition to facilitating situations of violence such as school and sexual harassment. Furthermore, mobile devices have become a gateway to pornographic content, which generates a trivialization of sexual relations, early sexualization and exposure to inappropriate content. Finally, the signatories also warn about the massive collection of data from minors, with a view to profiling them for sale to third parties for advertising purposes.

The proposed measures emphasize the need to assume the problem, train professionals to deal with it, and develop current legislation so that all actors involved assume their responsibility towards a vulnerable population such as children and adolescents. The proposals concern various levels of Public Administration.

#### ÿ 3.6.2 Video updates

##### Protect your privacy: Whatsapp, Instagram, TikTok

The AEPD updated its Instagram privacy and security configuration videos in 2023, **TikTok** and **WhatsApp**. The videos begin with a brief introduction explaining what each service is and what it is used for. Next, they make a tutorial that guides users step by step through the privacy and security configuration options of each of these services, offering recommendations to opt for the highest degree of privacy possible.



### 3.6.3 Specific broadcast of the Channel priority and responsibilities that may be incurred when disseminating sensitive content, and those that can have to respond jointly fathers and mothers

At the end of September 2023, a case of photos manipulated with artificial intelligence that showed naked girls was known, using the real faces of the young women and fake bodies generated with Artificial Intelligence. This is what has been called sexual deepfakes; a practice that has become popular thanks to new technological tools available to anyone and that can involve a violation of data protection regulations and even a crime.

The impact that this case had in the media and the press queries raised with the Agency led to the specific dissemination of the Priority Channel (to request the urgent removal of the images if they had been published on Internet pages) and to the administrative responsibilities, civil and criminal penalties that the minors responsible for these images and their dissemination could have incurred. In addition, the Agency announced that it was launching an ex officio investigation.



**In this context, the visibility of the AEPD stood at a total of 452 news items.**

**The audience impact exceeded 92 million, with an economic return of more than 2.8 million euros.**

### 3.6.4 Collaboration with the Ministry of Public function

In March 2023, the Agency **made a video to promote public talent** with the participation of several workers at the Agency.

### 3.6.5 Dissemination of projects with FIIAPP

The Technological and International Innovation divisions participated in two projects together with the FIIAPP in 2023. The first leads the data protection component of the EU4DigitalUA project that the FIIAPP implements in Ukraine. The second participates in the digital alliance between the EU and Latin America and the Caribbean, which includes the European project Digital Policy Dialogues and Regulations, which includes the participation of AEPD personnel. This collaboration has resulted in several joint and coordinated online dissemination initiatives.

### 3.6.6 Promotion of the Priority Channel - March 8

On the occasion of International Women's Day, the Agency published the data corresponding to 2022 of the Priority Channel, calling on people to report the publication of sexual or violent content published without consent.

The figures revealed that **a large percentage of the interventions carried out in 2022 involved digital violence against women and girls, accounting for 70% of the cases** reported in the Priority Channel.

### 3.6.7 Collaboration with Eurochild

In March 2023, the Agency adapted two of the infographics from the Priority Channel into English at the request of Eurochild, which wanted to disseminate the information from this Channel in the working group they maintain with 26 organizations in 21 European countries to work on child safety and online teenagers. The objective, in addition to disseminating it as a good practice, is that these organizations can advocate for the establishment of a similar mechanism at the national level.

### 3.6.8 Agreement with RTVE

The Agency and RTVE signed an agreement that makes public service cooperation between the two institutions possible. Through it, RTVE collaborates in the dissemination of the activities organized by the AEPD that are considered of special relevance and interest, in addition to producing in its facilities, with its own technical means, the weekly space 'We protect your privacy' that is broadcast on Radio 5. Likewise, the spaces are hosted on the RTVE Play Radio digital platform.

### 3.6.9 Fourth edition of the online course 'Minors and safety on the Internet', organized by the AEPD, INCIBE and INTEF

The Agency, the National Cybersecurity Institute (INCIBE) and the National Institute of Educational Technologies and Teacher Training (INTEF) launched the **4th edition of the free online course 'Minors and Internet Safety'**, which took place from June 7 to 16. The Agency contributed to its dissemination, both through its website for minors, its social networks and its blog.

### 3.6.10 MOOC 'Educate in digital security and privacy' 2023

The Agency, in collaboration with the National Institute of Cybersecurity (INCIBE), dependent on the Ministry of Economic Affairs and Digital Transformation, and the Ministry of Education and Vocational Training, through the National Institute of Educational Technologies and Teacher Training (INTEF), carried out a free training course in MOOC format, aimed at teachers, during December 2023.

As with the one mentioned above, the Agency also collaborated with its dissemination, both through its website for minors, its social networks and its blog.

## 3.7 Dissemination campaigns

### Presentation of age verification criteria

In December 2023, the Agency presented an effective proposal for an age verification system and protection of minors on the Internet from access to adult content, demonstrating that it is technically possible to protect minors from access to content inappropriate for while the anonymity of adults is guaranteed when browsing

Internet.

The visibility of the AEPD in the context of the development of an age verification system to access online content for adults was immediate (period December 16-19), reaching more than 300 news items.

**The impact achieved exceeded 66 million, with an economic return of more than 2.2 million euros.**



### 'Change the plan' campaign

The Spanish Data Protection Agency and the Spanish Association of Pediatrics (AEP) launched their 'Change the plan' campaign in October 2023, an initiative to promote the digital health of minors through raising the awareness of their parents. reducing the risks posed on a physical, mental, sexual and social level by the intensive and uncontrolled use of screens. The campaign promotes the use of the **Digital Family Plan**, a platform with useful information on the appropriate use of digital media by minors for families and pediatricians.

'Change the plan' **had the support of the Atresmedia Foundation, Mediaset Spain and RTVE**, entities adhered to the **Digital Pact for the Protection of People** of the AEPD who broadcast the spot through their respective



channels, and who reinforced with their participation their commitment to the rights of children and adolescents in the digital environment. The television campaign had 66 screenings and almost 34 million impacts. The collaboration with the AEP, in addition to the campaign on television and social networks, was also reflected in a series of materials that appear in the Infographics section of this Report.

In addition, the 'En Plan' campaign **was sent to the following organizations**, so that they could contribute to its dissemination:

- Education Departments of the CCAA, Family and/or Social Rights Councils of the CCAA, including Ceuta and Melilla, INTEF, Andalusian Women's Institute, General Education Commission, State School Council, Data Protection Delegates of Education.
- Parent Associations: State Foster Care Association, ATENEA Foundation, Association of Families for Coexistence, Association of Homoparent Families, Association of Lesbian and Gay Families, Federation of Associations of Single Mothers, Isadora Duncan Single Parent Family Foundation, Union of Family Associations, Women's Foundation, Gender Violence Observatory.



### • 'More than a mobile' campaign + The guide that does not come with the mobile with UNICEF Spain

The Agency and UNICEF Spain launched their '**More than a mobile**' campaign in November 2022, aimed at offering families the keys they should take into account before giving their sons and daughters a mobile phone. The More than a mobile website has received more than 130,000 queries since its launch. For its part, The guide that does not come with the mobile phone, the most notable material of the campaign, has obtained **more than 350,000 downloads**.

At its launch, the campaign had the collaboration of Movistar, Orange, Vodafone, Yoigo, Fundación Atresmedia, Mediaset España, RTVE, JC Decaux, Metro de Madrid and EMT Madrid, which distributed it for free through their respective channels, so that all families have access to basic advice on how they can prepare their sons and daughters for access to these technologies.

The cumulative impact of the campaign was **more than 300 million impacts**, to which we must add the support provided by META through its social networks (Instagram and Facebook) to spread the campaign. This investment made by Meta materialized in advertising credits assigned to UNICEF to be spent on the promotion of 'More than a mobile phone', taking users to The guide that does not come with the mobile phone published on the Agency's website.

**Three main moments** were established for the use of these credits: the week of **January 9, 2023**, after the arrival of the Three Wise Men before the foreseeable gift of a mobile phone, the days

adjacent to **January 28**, international data protection day, and the days adjacent to **February 7**, safe internet day.



According to data provided by UNICEF, a total reach of 9,090,771 and 821,355 total interactions was achieved.

### Collaboration in the campaign One click away from helping them

The Agency collaborated in the **'One click to help them'** campaign of the European Association for the Digital Transition, an initiative in which the Atresmedia Foundation and the Anar Foundation also collaborate).

'One click away from helping them' tries to encourage a more active role of parents in the online activity of minors, warning of risks such as cyberbullying, lack of communication or self-esteem problems and also of the peculiarities of some business models of platforms and social networks, based on the profiling of minors' data.

The campaign spot was broadcast free of charge on all television channels (**Antena 3, laSexta, Nova, Neox, Mega, Atreseries**) and radio channels (**Onda Cero, Europa FM, Melodía FM**) of the Atresmedia Group since May 24. .



On television, 328 screenings were made, reaching 108 million viewers adults and on radio 172 passes of the wedge.

## 3.8 Prizes

### Awards granted by the AEPD

On January 26, 2023, the Agency presented the '2022 Data Protection Awards' in the Communication categories; Proactivity and good practices in compliance with the Regulations and the LOPDGDD; Good educational practices; Research 'Emilio Aced'; Entrepreneurship 'Ángela Ruiz Robles' and Good practices for greater protection of women against digital violence.

In the **Communication category**, the AEPD awarded the prize to the **Science and Technology Area of the EFE Agency** for its work on the risks of publishing images of minors on social networks by their parents; the implications of technologies such as artificial intelligence (AI) or biometrics for data protection, and the precautions that should be taken before scanning potentially malicious QR codes,

among other topics.

The jury awarded a second prize in this same category to **Maldita.es**, for the programs broadcast on its channel 'Maldita Twitchería', where subjects such as dark patterns and online manipulation were analyzed; identifying and addressing online harassment or the importance of encryption.

Regarding the **Award for Proactivity and Good Practices in compliance with the European Data Protection Regulation (RGPD) and the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD)**, in the category of companies, associations and foundations, the jury awarded the prize to the **Pro Bono Spain Foundation**, for its training program 'DataprotectiON Mode' for non-profit entities. The eminently practical project contributes to facilitating the understanding of data protection and offers templates, forms and practical tools to comply with the obligations set out in the regulations.

In the public sector entities category, the prize was awarded to the **Citizen Services, Transparency and Publications Division**.

**(DIVATP) of the Ministry of Science and Innovation**, for its training video project on personal data protection. These address, among other topics, regulations, the concept of personal data and data processing, the figures of the controller, data processor and data protection delegate, and the rights of the interested parties.

In the category of **Good educational practices in privacy and protection of personal data for safe use of the Internet by minors**, the jury awarded the prize in the category aimed at Primary Education, ESO, Baccalaureate and Vocational Training schools, to **Humanitas Bilingual School Tres Cantos** (Madrid) for their work 'Digital Mentors. 1st

Baccalaureate', a project through which 70 young people received training on the responsible and safe use of the Internet to subsequently work with students from the same center, from 5th grade of Primary to 3rd grade of Secondary School.

In the modality of commitment of people, institutions, organizations, entities, organizations and associations, public and private, the award was awarded to **Orange Spain** for 'A safe and responsible use of technologies', a project that offers online training courses related to education in new technologies and security, aimed at educators, parents, students and AMPAS, including training initiatives for students with special educational needs.

In the category of **Research in personal data protection** **Emilio Aced** the jury awarded the prize to **Guillermo Lazcoz Moratinos**, for his work 'AI systems in healthcare.

How to guarantee human supervision from data protection regulations', which highlights the

value of Artificial Intelligence (AI) in the healthcare sector taking into account human supervision in decisions and in the life cycle of the AI system.

Likewise, the jury awarded a second prize to **José González Cabañas, Ángel Cuevas, Rubén Cuevas, Juan López Fernández and David García**, for their work 'Unique on Facebook: Formulation and evidence of advertising (NANO) aimed at users with NO-PII data', where the authors analyze the user's level of identification in the social network with a number of data that does not directly identify them.

Regarding the category of **Entrepreneurship in personal data protection** **Ángela Ruiz Robles**, the jury awarded **Acuratio Europe**, for its 'Artificial Intelligence Platform to train neural networks while maintaining data privacy', a practical execution of the MIT approach (Massachusetts Institute of Technology) called vertical federated learning, which proposes the deconcentration of information in AI treatments in the training of neural networks.

Finally, in the category of **Initiatives and good practices for greater protection of women against digital violence**, the jury recognized the work of the **Cibervoluntarios Foundation**, for its work 'Stop, Think, Connect against Gender Violence', a training program in the safe use of the Internet focused on raising awareness and preventing different forms of gender-based digital violence in minors between 10 and 17 years old and their close teaching and family environment, through guided cyber training in educational centers throughout Spain.



## 5 Awards received by the AEPD

In 2023, the Spanish Data Protection Agency was awarded a total of seven awards, which are part of the 29 that the Agency has received in recent years for the actions carried out to protect people in a digital world.

### 1. Sustainable Justice Award from the 4th edition of the

**WLW Awards (Women in a Legal World)**, which recognize the work of individuals, companies and institutions.

The AEPD has received this recognition for its work in the fight against gender violence, as well as for promoting the constitution of a working group - of which the General Council of the Judiciary is a part - on this matter.

### 2. 2023 Internet Award for Personal Career.

The coordinator of the Support and Institutional Relations Unit of the AEPD, Jesús Rubí, was awarded by the Association of Internet Users (AUI) with the Internet 2023 award for Personal Career. The Jury took into account the work carried out by Rubí mainly in the AEPD within the framework of a constant process of evolution of economic activities and technological innovations with the focus on the fundamental right to data protection. Likewise, he highlighted that "his professional activity has focused on the search for realistic solutions that have contributed to a constant improvement of the right to privacy with transparency and guarantees for citizens."

### 3. 'Data Security and Protection Award' from the Digital Information Society Magazine.

The AEPD was awarded by the Digital Information Society Magazine with the award for the 'Security and Data Protection' candidacy of the Socinfo Digital 'AGE TIC' Awards, organized by the magazine with the aim of disseminating ICT development projects in the AAPP applied in citizen services and recognize the work of professionals in the sector.

The Jury highlighted that the project presented by the Agency provides an extensive vision of data processing and highlighted its value for growth and preparation in data and information security issues, as well as its benefit for society.

### 4. Social Responsibility Award from the 3rd edition of the ScreensAmigas Awards.

The Spanish Data Protection Agency was awarded in the Social Responsibility category of the 3rd edition of the ScreensAmigas Awards, for the actions carried out in the field of protection and promotion of the well-being of children in the digital field.

### 5. 'Conflict Resolution & Law Enforcement' Award from the Global Privacy and Data Protection Awards 2023.

The **Priority Channel** of the Spanish Data Protection Agency (AEPD) was awarded in the 'Conflict Resolution & Law Enforcement' category of the 6th edition of the Global Privacy and Data Protection Awards 2023, awarded within the framework of the 45th Global Assembly of Privacy, which brings together more than 140 data protection and privacy authorities worldwide. The award recognizes the value of the AEPD's Priority Channel as an effective instrument in situations in which the physical and psychological integrity of the affected people is put at serious risk by the dissemination of content published online that constitutes digital violence, especially against women, children and vulnerable people.

### 6. Award in the 'Innovation' category of the VI Confiflegal Awards:

The director of the Spanish Data Protection Agency (AEPD), Mar España, was awarded in the VI Confiflegal Awards in the 'Innovation' category. The jury valued "the work carried out in the field of data protection and privacy, advocating for legal and technological solutions to minimize the negative impact of misuse of the Internet and social networks, especially in the context of sensitive content and protection juvenile".

**7. QIA Award for 'Innovation in the public sector'.** The Spanish Data Protection Agency was awarded the Quality Innovation Award, QIA 2023 - awarded by the National Association of Centers Promoting Excellence (CEX) - in the category of 'Innovation in the public sector', for its project ' Practical initiatives to protect minors on the internet with healthy, positive and safe environments.' The QIA organizing committee considered the Agency's project as a quality innovation, an innovation that meets five characteristics: novelty, usefulness, learning, customer orientation and effectiveness.



The complete history of awards received by the AEPD can be consulted at this [link](#).

### 3.9 Access to public information and transparency

Transparency is one of the main values of this Agency, as a necessary requirement to guarantee its independence in the development of the functions entrusted to it.

Regarding active transparency, the AEPD complies with its obligations **through its own website** and applies the criteria of the Transparency and Good Governance Council. In 2023, there has been a 36% increase in the number of accesses to the Transparency section of our website.

Regarding access to public information, there has been a decrease in the number of requests, compared to 2022. However, the percentage of total concessions increases slightly.

Most of the requests refer to sanctioning files and resolutions, but access to legal reports from the AEPD, information on the number and type of Delegates of

Protection of Data communicated to this Agency,

the budget invested in institutional advertising, or on the personnel who provide their services at the Agency.

As in 2022, 100% of the access resolutions adopted by the AEPD have been issued within the legally established deadline for resolution.

Throughout 2023, 10 AEPD resolutions were appealed before the Transparency and Good Governance Council (CTBG), which represents less than 9% of the resolutions, and all of them have been rejected by the CTBG, thus confirming the resolutions of the Agency.

Of special interest is the resolution of the CTBG in which it confirms that, in a sanctioning procedure in progress, with the communication of the opening date of the sanctioning procedure, the maximum duration of the same, and the information that at the moment in which issues a resolution that puts an end to the procedure, a new communication will be sent to the plaintiff; The right to know the status of the procedure is considered fulfilled. Without recognizing their right of access to the rest of the information generated within the framework of an ongoing sanctioning procedure in which the applicant (complainant) does not have the status of interested party.

Likewise, it has also supported that there is no claim before the CTBG against a Resolution on access to public information when said information has been provided by the same organization in a right of access procedure subsequent to the one claimed.

Also noteworthy is the ruling of the CTBG regarding the inadmissibility of a claim when an appeal for reconsideration has been filed against it, given that article 23.1 of the LTAIBG configures the claim before the Council as a substitute for administrative resources, of which results in the impossibility of combining both routes simultaneously.

The Information and Transparency Unit (ITU) of the AEPD participates in the working group of the European Data Protection Committee preparing the European comparative study on access to documents from sanctioning proceedings

and cross-border research actions.

Likewise, the ITU of the AEPD participates in the working group that brings together all the ITUs of the General State Administration (AGE) for coordination of criteria, which is convened and directed by the DG of Governance. In application

of its commitment to transparent action, the AEPD **publishes on its website** the final resolutions denying, or partially denying, for general knowledge of the reasoning and motivation for their actions.

## 4. Effective help to entities

### 4.1 Obligated subjects and data protection delegates (DPD): operation of the DPD Channel and assessment of DPO queries

The obligated subjects, responsible and in charge of the treatment, must comply with the principle of proactive responsibility that is complemented with the obligation, in some cases or the possibility, in others, of designating a DPO, through which queries can be made to the AEPD.

Pursuant to article 39.1.e) of the RGPD and in accordance with the requirements set forth in rule 4 of Instruction 1/2021, the AEPD may be consulted by the DPOs, under certain requirements consistent with the principle of proactive responsibility. , and by the organizations and associations representing data controllers and processors that provide advisory services on data protection to their associates, especially when it comes to small and micro businesses, under the same conditions established for DPDs.

Regarding its content, the following can be highlighted as most relevant:

• **In the field of public security:** Issues related to video surveillance and the interpretation of Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of infractions criminal sanctions and the execution of criminal sanctions, have generated important doubts regarding the regulations applicable to the installation of fixed video cameras on public roads by the State Security Forces and Bodies. In these matters, the AEPD together with the rest of the autonomous authorities has interpreted that the requirement for authorization for the installation of fixed video cameras established by Organic Law 4/1997, of August 4, which regulates the use of video cameras by the Security Forces and Corps in public places and its implementing regulations remain in force, not having been repealed by Organic Law 7/2021.



The queries received amount to a total of **850**, which represents an **increase of 22.3%** compared to the previous year.

There continue to be numerous queries raised by the Local Police in which authorization from the AEPD is requested for the installation of cameras on the public roads of their Municipalities.

It is noted in any case that the AEPD does not have among its powers to authorize the installation of this type of devices, beyond pointing out the considerations that must be taken into account.

account at the time of installation and which can be consulted on the Agency's website in the section dedicated to [video surveillance](#).

🔗 **In the workplace**, the implementation of facial and fingerprint recognition systems as a measure for workers' time control and access control continues to be a recurring issue. The publication of the "CEPD Guidelines 05/2022 on the use of facial recognition techniques in the field of law enforcement" has had a special impact on these issues, making it clear that with technological evolution it is necessary to establish greater controls for both authentication and identification based on biometric elements of the person, and consider the limits to the processing of biometric data and the measures that must be established so that a processing of personal data that decides to use biometric systems Ensure GDPR compliance.

On these issues, the AEPD has published a [Guide on presence control treatments using biometric systems](#).

establishing the criteria for the use of biometrics in the registration of working hours or access control for work and non-work purposes.

🔗 **In relation to unwanted advertising**: With the entry into force of Law 11/2022, of June 28, General Telecommunications, numerous queries have also been raised regarding the interpretation that should be given to its article 66.1. b), in relation to the legitimacy for the processing of data in unwanted calls for commercial communication purposes, especially with regard to the possible legitimate interest admitted by said provision. On this issue, the Agency has approved [Circular 1/2023, of June 26, on the application of article 66.1.b\) of Law 11/2022, of June 28, General Telecommunications](#).

🔗 **Regarding the fight against corruption**: The publication of Law 2/2023, of February 20, regulating the protection of people who report regulatory infractions and the fight against corruption, is also being the subject of consultations because of its processing of personal data is derived from the application.

Mainly, these are issues related to the implementation of internal complaints systems in the environment of Public Administrations and related to the legal position of each intervener (assignments of roles of data controller, managers or co-responsible). Regarding the general principles of the internal information and defense system for informants, and the information management procedure provided for in Law 2/2023, the AEPD has approved and published the [Principles of the internal information and defense system for informants](#), and the [Procedure for information management of Law 2/2023](#).

## 🔗 4.2. Registration of Data Protection Officers

The importance of the role of data protection officer (DPO) as a fundamental element for compliance with the RGPD is evident as can be seen from the functions, position and characteristics attributed to him by both the RGPD and the LOPDGDD.

The AEPD has continued to promote the provision of tools, resources and communication channels to the people who perform this function so that they can carry out their function with guarantees of solvency and independence. At the same time, the AEPD has also continued with the work of raising awareness among those responsible for the designation of DPD, as well as those who consider their designation on a voluntary basis, to provide this figure with sufficient resources to carry out the tasks that the GDPR attributes to them.

It has also participated in the coordinated European action to analyze the designation and situation of data protection delegates in public and private entities, within the framework of coordinated actions of the CEPD. This action has resulted in a report that offers a vision of both the public and private sectors in order to contribute to raising the level of compliance and protection of citizens' personal data throughout the EU.



**In execution of this coordinated action, the AEPD has analyzed the practice of more than 10,000 entities in the public and private sector.**

These entities responded to the questionnaire sent and which included questions about the designation, knowledge and experience of the DPOs, their tasks and resources or their role and position in their respective organizations.

The recommendations collected have pointed out the need to continue promoting awareness among organizations so that they adopt the necessary diligence in the appointment of the DPO; that those responsible verify the means made available to the DPOs so that they can effectively carry out the functions entrusted to them; to provide training and education of DPOs through various mechanisms, as well as encourage the use of certification; to provide the DPD with due independence in the exercise of its functions in order to avoid conflicts of interest as well as promote the visibility of this function within the organization; the importance of promoting internal mechanisms for the DPD to report to the highest level of the organization; to continue with the work carried out so far by the supervisory authorities in order to provide guidelines and tools that contribute to the effective performance of said functions.

### § 4.3. Meeting with the DPD of the Public Administrations

As a continuation of the meetings held with the DPOs of different Public Administrations and sectors of activity in 2022, and within the framework of the consultative function provided for in Instruction 1/2021, on March 28, 2023, the meeting with the DPD of the local entities belonging to provincial capitals and cities of 100,000 inhabitants and of the Provincial Councils, Cabildos and Island Councils within the scope of competence of the AEPD.

This 6th Meeting, held after the pandemic, with the aim of maintaining a space for continuous dialogue with the DPOs, as key elements of the public sector data protection ecosystem, as well as knowing through the DPOs themselves what the situation is. current with respect to the exercise of their functions and exchange experiences and good practices developed in the sector. Furthermore, it is of utmost importance to support the work of DPOs and reinforce their independence from those responsible for the treatment.

At this Meeting, the results of the survey on the status of the DPOs in the Local Entities were addressed, among whose results stand out their performance both as DPOs in charge and in charge, in the case of the DPOs of the Provincial Councils, their designation based on their knowledge and experience, and 58% perform their task part-time, combining it with other tasks of a different nature, the absence of an annual report provision (38%) and the interest in receiving materials from the supervisory authority. for the best performance of their functions.

Likewise, the presentation of the thematic area dedicated to the Public Sector enabled on the AEPD website, personal data breaches, the most relevant sanctioning procedures in the field of local entities and the [Priority Channel took place.](#)



Finally, the queries raised by the attendees prior to the celebration of the Meeting were addressed, as well as those that arose throughout the meeting. Among these issues, general considerations regarding access to the Register data were addressed, as well as doubts regarding the processing of contact data of individual entrepreneurs and liberal professionals; the use of so-called onboard cameras by local police, as well as the use of non-corporate mobile phones by local police; use of the Municipal Register of inhabitants by the City Council to carry out a consultation on municipal investment projects; dissemination of images of associations of older people or groups of minors who visit the City Hall; access to the registry data of your minor child for whom you have parental authority in the case of separated parents.

## ÿ Coordinated action of the European Data Protection Committee on the designation and situation of DPOs

During 2023, the Spanish Data Protection Agency has participated in the second coordinated action of the European Data Protection Committee, which aimed to analyze the designation and situation of DPOs in organizations, whether they occupy the position required by the RGPD and whether they have the necessary resources to carry out their tasks.

In developing this action, the AEPD analyzed the practices of the more than 10,000 public and private sector entities that responded to the questionnaire sent and which included, among others, issues related to the designation, knowledge and experience of DPOs, their tasks and resources or their role and position in their respective organizations.

Within the framework of the private sector, the questionnaire was addressed to different sectors of activity: education, banking and financial entities, health, energy sector, security, telecommunications services, asset solvency and credit, and activities related to games of chance and betting. .

Action in which the Transparency and Data Protection Council of Andalusia has collaborated in its scope of action.

The final report of the CEPD (adopted at the beginning of 2024) includes a series of **recommendations and points of attention** aimed at organizations, DPOs and supervisory authorities, such as as:

- ÿ Continue promoting awareness among organizations so that the designation of the DPO complies with those provided for by the RGPD.
- ÿ The need for data controllers to verify that the means made available to DPOs allow them to effectively carry out the functions entrusted to them.
- ÿ Provide training and education of DPOs through various mechanisms, and promoting the use of certification.
- ÿ The need to guarantee the independence of the DPD for the exercise of its functions in order to avoid conflicts of interest, as well as promote the necessary visibility of the delegate within the organization.
- ÿ The importance of promoting internal mechanisms and processes so that the DPD reports to the highest level of the organization.
- ÿ Provide control authorities, as until now, with guidelines and tools and resources that contribute to the effective performance of DPD functions.

#### 4.4. DPD Certification in accordance with the AEPD-DPD Scheme

Article 37 of the GDPR establishes the figure of the data protection officer (DPO) as one who, among other activities, must advise data controllers on compliance with data protection legislation, in addition to including the requirements that must comply with said DPO, since it establishes that "he will be appointed based on his professional qualities and, in particular, his specialized knowledge of law and practice in matters of data protection."

The AEPD, with the purpose of facilitating the designation of qualified DPOs by those responsible for the treatment, saving time and resources, developed in July 2007 a Certification Scheme in line with the provisions of article 35 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.



**In 2023, the main magnitudes of the Scheme have to do with the number of certified DPDs, which have been 169, 42 % of the 404 candidates to obtain it in a total of 62 tests.**

With them, the total number of DPOs that have obtained certification under the AEPD Scheme as of December 31st amounts to 1,100, a figure that contrasts with the number of DPOs that have been reported to the AEPD (10,459), if it clearly shows that the percentage of certified DPO over the total DPO continues to increase, reaching 10.52% (9.67% the previous year).

After the strong impact of the pandemic, which produced a downward trend in the number of DPOs certified in those years, 2023 has represented a reversal of the trend and it is observed that it is the first time that the number of DPOs certified during the year exceeds to the previous one.

Another relevant aspect has been the withdrawal of one of the certification entities from the Scheme, so there are currently 7 certifying entities accredited by ENAC.

Regarding training entities, the AEPD has recognized the University of the Basque Country as such for its Master in "Personal Data Protection, Cybersecurity and ICT Law" which is added to the two previously recognized Universities.

#### 4.5. Codes of conduct

In 2023, in accordance with the provisions of the RGPD, the development of codes of conduct has continued to be promoted with the aim of contributing to their correct application, taking into account the characteristics of the data processing carried out according to the sectors of activity.

Likewise, and in compliance with the provisions of the second transitional provision LOPDPGDD, the process of adapting the standard codes continues.

To this end, numerous meetings and contacts have been held with the promoters of codes of conduct whose projects are in the pipeline with the aim of adjusting their content to the requirements of the RGPD, CEPD Guidelines 1/2019 and the accreditation criteria of the supervision bodies adopted by the Agency, which implies the study and assessment of the projects presented and their successive versions and, where appropriate, making recommendations and suggestions for improvement. In some cases, and as in previous years, the collaboration of other AEPD units has been requested in those sections that deal with matters that make up their daily work.

It is important to highlight the Agency's drive to develop codes of conduct that regulate extrajudicial procedures and other conflict resolution procedures that allow for the resolution of disputes between those responsible for the treatment and the interested parties related to the treatment, without prejudice to the rights of the data subjects. interested parties under articles 77 and 79 (art. 40.2.k GDPR).

## ÿ National codes

The total of codes approved by the AEPD so far are listed below:

- ÿ **“Code of conduct for data processing in advertising activity”** promoted by AUTOCONTROL and which has been modified in 2023 fundamentally due to the need to adapt it to the regulatory changes of Law 11/2022, General of Telecommunications. nications and the LOPDPGDD, as well as the provisions of the AEPD Circular 1/2023.
- ÿ **“Code of conduct regulating the processing of personal data in the field of clinical trials and other clinical investigations and pharmacovigilance”** promoted by FARMAINDUSTRIA.
- ÿ **“Code of conduct regulating the processing of personal data in common systems of the insurance sector”** promoted by UNESPA.

Regarding these three codes, point 6.1 of the Accreditation Criteria for code of conduct supervisory bodies establishes that *“The supervisory body will report annually to the AEPD on the activities carried out, which includes both the measures and procedures carried out. to verify compliance with the code, and its results, such as the complaints received and their results.”*

In accordance with this criterion, the activity reports corresponding to the approved codes have been received, and their analysis has been carried out to verify compliance with what is established therein.

Currently , **16 draft codes of conduct** are in different stages of processing, **9 referring to the adaptation of standard codes and 7 to new projects.**



At the time of closing of this Report, the processing of the “Code of conduct for the resolution of data protection disputes in the electronic communications sector” promoted by the following teleoperators is very advanced: Orange Espagne, SAU, Orange España Virtual, SL, Telefónica de España, SAU, Telefónica Móviles España, SAU, Vodafone España, SAU, Vodafone ONO, SAU, Xfera Móviles, SAU and Pepemobile, SL

## ÿ Transnational Codes of Conduct

In addition, the AEPD has participated in the processing of 5 draft codes of conduct led by data protection authorities of other Member States within the framework of the coordinated procedure.

In fiscal year 2023, the AEPD acts as a co-reviewing authority in the EU CODE OF CONDUCT ON SCIENTIFIC RESEARCH project, promoted by the European Federation of Pharmaceutical Industries (EFPIA).

Likewise, the AEPD has reviewed the latest version of the EUCROF code of conduct, led by the French Authority, and has made observations to the consultation formulated by the Austrian Authority in relation to the code for Cross-border Marketing by postal mail.

## 4.6. Promotion of the fundamental right to data protection

The AEPD, within its promotional function, carries out awareness-raising actions aimed, on the one hand, at data controllers and processors about the obligations incumbent on them under the RGPD and the LOPDPGDD and, on the other, at the public, which includes understanding the risks, rules, guarantees and rights in relation to the processing of your data, which are developed through courses, conferences and participation in events that have the purposes described.

The AEPD offers two types of courses:

- 20-hour course configured in **8 videoconferences in online format.**
- **6-module course in Moodle format.** A live videoconference has been incorporated into each of the modules, for greater interaction between students and teacher.

In addition, more specific courses are taught, adapted to the characteristics of the data processing activities of specific organizations and entities, subject to the availability of the AEPD.

The training provided during 2023 **has been aimed at:**

### • The General Administration of the State.

- **Ministries:** Health; Social Rights and Agenda 2030; Transport, Mobility and Urban Agenda; Inside; Education and Vocational Training; Work and Social Economy; Inclusion, Social Security and Migrations; Territorial Policy; Justice; Defending; Ministry for the Ecological Transition and the Demographic Challenge.

- **Other public bodies:** Court of Accounts, University of Las Palmas de Gran Canaria and Principality of Asturias.

### • Courses aimed at public employees.

They are organized by the National Institute of Public Administration (INAP), on the "Application of the General Data Protection Regulation in Public Administrations", and are taught by representatives of the AEPD, which have had 600 students.

It is worth highlighting the "Specialized program for data protection delegates of Public Administrations.", a specific course to train future DPDs and whose first edition had a new methodology, structure, etc.

The "Specialized program for data protection delegates in Public Administrations" was taught to **80 students** during the first semester of the year.



An important aspect of the promotional activities are those aimed at disseminating the measures adopted by the AEPD for the protection of vulnerable groups against situations of digital violence, particularly the Priority Channel. In 2023, **we participated in various Conferences organized by:**

- Diagram Foundation
- Violence against Women Unit, Government Subdelegation in Segovia
- Ministry of Justice

In addition, a Regulatory Quality Conference on data protection was held, where topics such as the Agency's advisory role in the development of standards and the Regulatory Impact Analysis Report (MAIN) were addressed; risk analysis and impact assessments on data protection in normative production, and the impact of the General Data Protection Regulation on the content of the guarantees to be incorporated into the standard.

## 4.7. International transfers

During 2023, once the European Data Protection Committee issued its favorable opinion, the AEPD has approved the binding corporate rules (BCR) of the multinational group Prosegur.

During this period, the Align Technology group has requested that the AEPD act as the leading authority with respect to its BCR (responsible and in charge).

Although these BCRs were already adopted at the time by the authority of the Netherlands, a change of lead authority has been requested due to the designation as the main entity of the group to an entity established in Spain.

The total of BCRs adopted by the AEPD at the end of this period is 10 binding corporate standards.

Currently, 12 BCR projects are in different stages of processing within the framework of the coordinated procedure and consistency provided for in the GDPR. At the time of closing of this Report, the BCRs of Mapfre and Telefónica are in the final processing phase.

In addition, the AEPD has participated as a co-reviewing authority in the processing of 4 BCR projects led by data protection authorities of other Member States also within the framework of the coordinated procedure.

# 5. The power of supervision

## 5.1 Results

The greater presence and scope of personal data processing in society and the consequent concern of citizens about the processing of their data is once again reflected in the record of complaints before the Agency, which once again reaches a record volume. precedents.

than during the year 2022. Despite this, the large increase in entries has had its impact on the complaint resolution rate - which compares the number of complaints received with the number of complaints resolved in the same year - which has dropped to 94% compared to 99% the previous year.

Regarding the activities carried out by the SGID, it can be highlighted that the GDPR establishes among the Agency's functions that of processing the complaints submitted and investigating them to the appropriate extent, informing the complainant about the course and the result. This is carried out in the SGID through the actions and procedures that are regulated in Title VIII of the LOPDGDD and, additionally, in the regulation of the common administrative procedure established by the LPACAP.

The processing of claims begins with an evaluation of admissibility that includes a first phase of prior analysis of admissibility, to subsequently develop the phase of transferring the claim to the person responsible or in charge and deciding on its admission for processing.

Once admitted for processing, if it is deemed necessary

**In 2023, 21,590 claims were registered, 43% more than the immediately previous year. In the three years of this decade, the complaints that the Subdirector General of Data Inspection (SGID) has to process have doubled.**



During the year 2023, more claims have been resolved than in any previous year, being 37% more

To determine the circumstances of the infraction and complete the identification of the person responsible, prior investigative actions are carried out, to finally consider the convenience of initiating the sanctioning procedure or the warning procedure. In the event that the claim is related exclusively to the rights established in articles 15 to 22 of the RGPD, with the admission of the claim for processing a specific procedure for the exercise of rights can be initiated.

It should be noted that in the last two years the criteria that advise the opening of investigation actions prior to the initiation of the procedure have been revised, which has led to a reduction in the number of investigations since then, thus allowing inspectors to dedicate more time to investigations that have a greater impact. This trend continues in 2023, improving the effectiveness of the work carried out by the SGID given that of the investigations carried out: 55% culminate in the opening of the procedure, compared to 39% in 2022, and 28% in 2021 .

Through the indicated actions and procedures, other types of entries are also processed, other than the claims themselves submitted to the Agency, and which did not exist prior to the application of the RGPD: cases from other control authorities of the European Economic Area (EEE) and notifications of personal data breaches in which the SGID investigation proceeds. Also emerging in recent years is the priority channel for the removal of sensitive content, such as photographs, videos or audios of sexual or violent content that are published on the Internet, which may cause irreparable damage to the rights and freedoms of those affected. This channel also includes specific access for minors between 14 and 18 years old. All of this, together with the actions carried out on their own initiative, add up to more than 1,250 additional entries in 2023 to the claims that also give rise to the actions described.

In addition to the powers that the Agency has derived from the RGPD and the LOPDGDD, General Telecommunications Law 11/2022 (hereinafter, LGTel) and Law 34/2002 on Information Society Services and Electronic Commerce (hereinafter, LGTel), hereinafter, LSSI), as special laws, also grant powers to the SGID to apply the procedures provided in Title VIII. Apart from these two regulations, various laws have been approved in this decade that also empower the Agency and, in particular, the SGID, to intervene by controlling and supervising the application of certain provisions.

Among them are Organic Law 1/2020, of September 16, on the use of data from the Passenger Name Registry for the prevention, detection, investigation and prosecution of terrorist crimes and serious crimes, the Law Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal infractions and execution of criminal sanctions, Organic Law 8/2021, of May 4 June, on comprehensive protection of children and adolescents against violence, which have a direct impact on the activities of the SGID, Organic Law 10/2022, of September 6, on the comprehensive guarantee of sexual freedom, or the Law 13/2022, of July 7, General Audiovisual Communication, to name the most significant. These new assignments result in an increase in entry, with claims that come from different regulatory areas with their own peculiarities that should be distinguished when carrying out the procedures.

In short, all of this contributes to a **trend of increasing claims and the work of the Agency**, which will foreseeably continue to occur in the coming years due to the persistence of the causes that produce it.

It is also worth mentioning the 6% increase in reconsideration appeals filed against procedural resolutions, after having also increased significantly in previous years (13% and 18% in 2022 and 2021 respectively), which It represents an increase of more than 40% in three years.

Analyzing now the acts that put an end to the actions of the SGID, almost 70% of the claims received end after the prior analysis of admissibility and, therefore, do not continue to subsequent phases.

It is necessary to highlight the exceptional nature of the sanctioning procedure, which is why, when possible, alternative mechanisms covered by the regulations are chosen, as occurs with the referral of the claim to the DPD or to the person responsible or in charge, as provided by the article 65.4 of the LOPDGDD. Taking as a reference the claims that exceed the prior claim analysis, that is, 30% of the claims, it is observed that only 8% of the resolutions occur in the sanctioning procedure, compared to 86% that occur after the transfer. of the claim. Thus, the main way of resolving complaints is by sending them to the person responsible or in charge of processing, who analyzes the complaint and provides a response to the Agency which, in a significant number of cases, allows us to conclude that there is no infringement or that This has been corrected, and it is not considered necessary to open new actions, regardless of the investigative and sanctioning powers that the AEPD can always initiate.

These mechanisms also have a reflection on the times in which citizens obtain a response to their complaints, which has decreased since they began to be applied. However, in this last year, after several years of successive reductions, the average resolution time for claims that exceed the previous admissibility analysis has increased by 3%, due to the large increase in claims received and the consolidation of the processes since the RGPD and the LOPDGDD are applied. However, the times are still low and citizens have seen their claim attended to in shorter periods than they would have had to wait if one of the procedures established in the LOPDGDD had to be initiated.

From the analysis of the data by classification groups, one more year it is observed how the claims

The most frequent complaints are repeated with those of the previous year (although in a different order): those related to advertising, internet services and video surveillance, together accounting for 46% of the total complaints. The increase in complaints related to advertising stands out mainly, with an increase of 114% compared to the previous one. In relation to this, at the end of 2022 work was done on the modification of the Autocontrol advertising code of conduct, to which the main telecommunications operators were able to adhere at the beginning of 2023, for the intermediation and rapid resolution of complaints about advertising. Unwanted.

Continuing with the classification groups, there has been a significant increase in complaints received regarding commerce, transport and hospitality (+66%) and, within this area, the increase in reported infractions related to the use of data by delivery and parcel companies, something that already happened during the previous year: for the most part these are claims associated with the delivery of parcels to third parties (neighbors or nearby stores) without having been informed about it, and thus revealing personal data of the recipients that are noted on the package label. Finally, it is worth highlighting a significant increase (+73%) in claims related to financial entities or creditors, mainly related to the exercise of rights.

In relation to sanctioning procedures and fines, the most frequent area of the former is video surveillance (164 procedures), although the largest volume of fines corresponds to cases related to personal data breaches. This is explained by the generally smaller nature of video surveillance cases, both due to their severity and the type of person responsible (natural persons) and their relationship with the effectiveness of the fines (in terms of proportionality). and deterrence capacity), in the face of the great impact of infringements with the presence of large companies in the field of personal data breaches that affect a large number of clients or citizens.



**The largest fine imposed in the year corresponds to a procedure in the financial institution sector, in which Caixabank SA is imposed, for violation of articles 5.1.f, 25 and 32 of the RGPD, a fine of 5 million**

**euros,**

in addition to ordering the necessary measures to correct the infringement and prevent its reproduction in the future.

Looking at the classification groups in terms of the volume of fines imposed, a decrease (-91%) in the amount of fines for the internet services group also stands out, which is explained by the previous year's procedure against Google LLC that involved alone a fine of 10 million euros.

At the European level, within the cooperation mechanisms between the control authorities of the States of the European Economic Area (EEA) for the management of cross-border cases, the increase in cases in which Spain acts as the main authority can be highlighted. , because the person responsible is established on national territory, such as cases of cooperation in which Spain acts as the interested authority. In total, cases have increased by 51%.

As for entries from other EEA states, they stabilized with a slight increase of 1%. The entry of new cross-border cases and consultations from other authorities increase, but the draft decisions of cases in which the AEPD participates are reduced. Given that in this last case it is a complex process that can last several years, the decrease in decisions in the year depends on the initiation of cases in previous years.

At the European level, the SGID has participated in several working groups to unite criteria and cooperate in various matters, as detailed in the Agency in Figures section of this Report. The participation that the SGID has had in the preparation of the draft fine-tuning of the GDPR aimed at cross-border cases is notable.

Likewise, we must also mention the obligations that the SGID has in relation to the supervision of the protection of personal data of the various agencies of the European Union and its large information systems, which serve the purposes of cooperation between the Member States, particularly in the judicial, police, and customs and border control fields. The data protection rules of each of them are found primarily in their respective establishment rules, which normally take the form of an EU Regulation, without prejudice to the fact that they are also applicable, depending on the material field in which the agency operates or system, the General Data Protection Regulation (GDPR) and the Criminal Matters Directive (DAP).

The audits of these large systems are being implemented gradually and, although the deadline for each one may differ between three or four years to complete them, their evaluation is carried out continuously.

Within the framework of the Schengen 2021 evaluations-2025, audits have been carried out on large EU information systems such as the Visa Information System (VIS), the Schengen Information System (SIS II) and EURODAC. Thus, regarding the VIS, inspections have been carried out, among other things, in the Consular Section of the Spanish Embassy in the United Arab Emirates, in the General Commissariat for Immigration and Borders, or in the Consulate General of Spain in New York. In relation to SIS II, among others, the Headquarters of Technical Services of the Civil Guard, the Liaison Office of the Schengen Information System and the Security Technology Center of the Secretariat of State for Security of the Ministry of the Interior have been inspected. Inside.

Finally, this year 2023, a new major European infrastructure system has been included in the list: EURODAC.

The greatest activity of the year has been dedicated to the preparation of the audits, studying the system and its specific regulations, and at the end of the year the first inspection took place of the General Commissioner of Scientific Police of the National Police, responsible for the National Access Point to EURODAC.



Finally, among the annual results, reference must be made to **the Agency's Priority Channel to request the urgent removal of sexual or violent content published on the Internet without consent.**



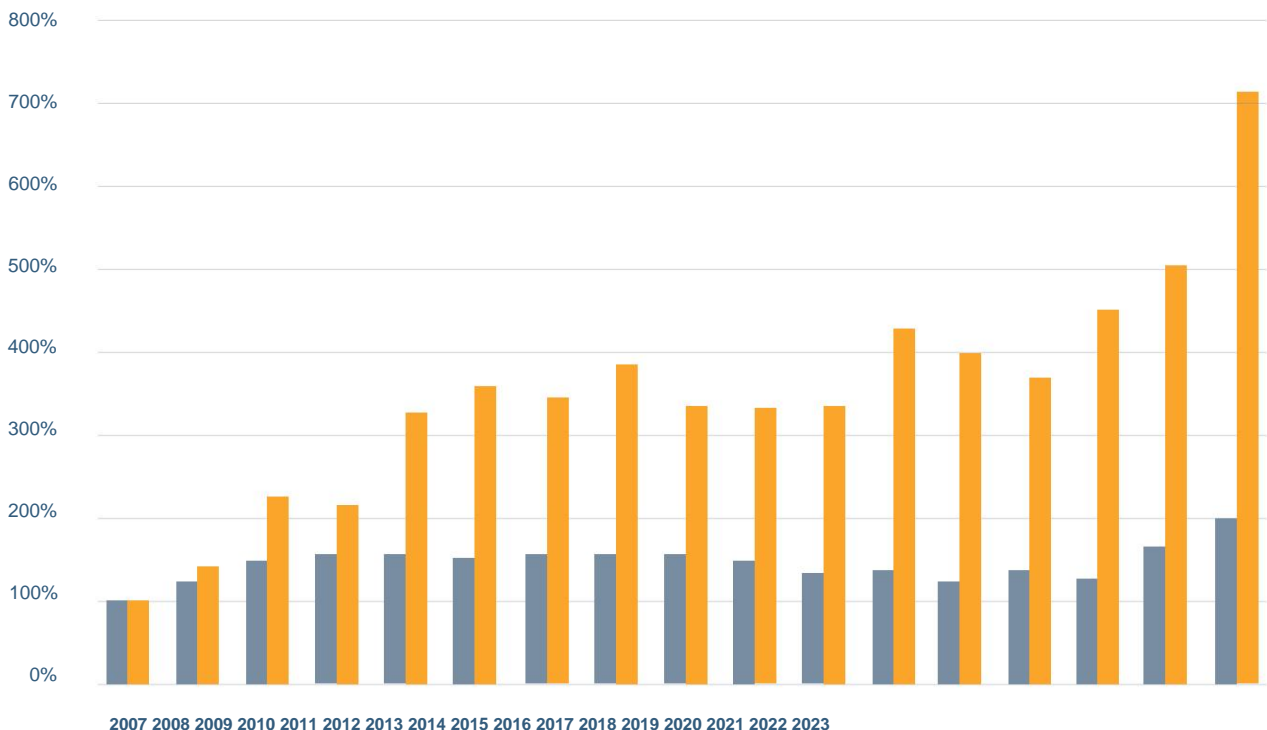
The number of entries received through this channel has increased by 36%.

However, if the Agency's previous analysis of these cases is taken into account, the number of entries that have actually been processed as urgent has been 32% lower than the previous year. The effectiveness rate of interventions, measured by the proportion of withdrawals

of content required and those actually fulfilled during the year have been 94%. The precautionary measures that have not been effective during the year were signed during the last days of 2023, therefore at the end of the year they are pending compliance, highlighting that the rest of the measures issued during the year have been 100% effective. %. However, during the first days of 2024 these measures were complied with, so it can be said that the effectiveness in compliance with the urgent content removal measures carried out during 2023 has had 100% compliance.

The complete detail of the volume of procedures carried out by the General Subdirectorato de Data Inspection and their assessment has been included in the section of this Report called The Agency in figures.

### Comparative evolution of the number of entries and SGID personnel, 2007-2023



Input evolution

Evolution of people working at SGID

To avoid the overflow and consequent collapse that the entire workload that has been reflected in the previous paragraphs can produce, among which a 43% increase in claims in a single year stands out, the Agency is developing from several strategies for coping with work a few years ago. They are based on three fundamental pillars: workforce adaptation, simplification and automation and regulatory modifications.

The first is the adaptation of the personnel.

In this case, the creation of new positions is a fundamental aspect: in 2022, 14 people joined and during this last year, 2023, another 17 have joined.



In this way, today this subdirectorate has **twice as many workers as there were in 2007. But the claims received are growing at a much higher rate, being seven times those received that year.**

The previous graph compares the growth rate of staff, compared to the number of entries that generate new files (mostly complaints before the AEPD, but also cases received from other authorities in the European area, priority channel for minors, notifications of security breaches in which an investigation is opened, and other cases of own initiative).

In addition, the increase in the number of complaints must be taken into account another trend that has been common, which is a greater extension of the scope of complaints and infractions investigated, with a lower presence of individual cases and a greater presence of cases that affect a generality of those affected, actually or potentially, by deficiencies in the personal data processing procedures. This greater scope is also reflected in the breadth of the actions that the SGID develops in response to these cases, which no longer require the investigation and correction of a

particular case, but the analysis and adaptation of the responsible person's procedures to what the regulations require. Which implies that the previous research actions that have been carried out have a much greater complexity, given that analyzing a particular case is not the same as a case in which there may be a bad design, which can affect a multitude of people.

Therefore, it is important to adapt the workforce to the workload. When incorporating new personnel into the Agency, it must be taken into account that the protection of personal data is a very specific topic and it is very difficult to find specialized personnel. **All new hires have received a two-month introductory training for the development of their work**, in addition to the Agency's own annual training plan, which includes some specialized courses.

In parallel with the incorporation of new personnel, it has been necessary **to reorganize the subdirectorate** by providing more personnel in the areas of evaluation of the admissibility of the claim to avoid collapse at the entrance due to the high volume of claims, allowing the claims and be able to decide within three months on their admission for processing.

However, this restructuring has caused the areas that carry out the procedures, including the sanctioners, to have been reduced in personnel, which causes a **problem in the medium term that is pending to be solved with the incorporation of new people during the year 2024.**

The second axis in which work has been done to adapt the workload has been **automation**. During 2023, automation has been added to various steps of the SGID procedures, both based on information systems and dynamic document modeling, with the aim of reducing processing times.

The first robotization processes have been put into practice for repetitive and mechanical tasks that had been done during the processing of

certain files. These changes do not represent a significant reduction in the workload, but they serve to relieve staff of mechanical tasks, allowing them to dedicate themselves to other activities in which the intervention of professionals is necessary. Additionally, other techniques continue to be evaluated for their future incorporation in different auxiliary tasks to the procedures.

Finally, related to simplification and automation, during this year 2023 we have worked on the **design of a new complaints mailbox in the electronic headquarters of the AEPD.**

This mailbox aims to facilitate the submission of claims to citizens, as it guides them by indicating the different documents they must present and asking the necessary questions so that the claim is complete. The mailbox, in addition to being one of the recommendations of the regulations, allows a better classification of the claims received and catalogs the documents provided, which results in an improvement in the work that the SGID must carry out. It was launched in the last days of the year, starting with complaints of unwanted advertising, one of the areas where the greatest number of complaints occur year after year, increasing in 2023 since the application of the obligations of the new General Law Telecommunications for commercial calls.

The third major axis on which work has been underway is that of regulatory modification. During 2023, modifications to the LOPDGDD have been approved, which give better coverage to the procedures for responding to claims. Among the modifications, it is worth highlighting the **creation of the warning procedure**, the regularization of the possibility of carrying out remote investigations or the possibility of establishing models for submitting mandatory claims. The warning procedure is a new procedure and totally different from the sanctioning procedure, which allows, in addition to warning the person responsible, if necessary, to include corrective measures, as in the rest of the procedures defined by the LOPDGG.

The LOPDGDD provides, in its twenty-third Additional Provision, that the AEPD may establish models for submitting claims in all areas in which it has jurisdiction, which will be mandatory for interested parties regardless of whether or not they are required to interact electronically. with public administrations. By virtue of this power, the Agency has established in 2023 a general model for submitting claims and six specific models referring to different processing of personal data, approved by **resolution**. from the director on June 29, 2023. Among the specific models is the one intended for cases of neglect by the person responsible for processing a request to exercise rights; as well as those reserved for cases of receiving unwanted direct advertising; installation of video surveillance devices; breaches in the processing of data linked to debts; priority channel and personal data breaches.

With this resolution, citizens are provided with the information they must include in their claim to be effective.

## 5.2 Most relevant claims and procedures

**In 2023, the increase in claims stands out especially received in relation to the receipt of unwanted advertising, which increased by 114% compared to 2022 and are ranked first in terms of the main group of activity with 20% of the complaints received.**



Of these, the majority refer to **unwanted commercial telephone calls**, as is the case of **procedure PS/00040/2023 against BOX 24 2050 SL**. This file begins with a claim for the reception of commercial calls from ROMBOC SL, an entity that has the energy consumption data of the complainant, and to which it has not given its consent.

As a result of previous investigation actions

It is evident that this company uses the database of CONCENTRA CENTRAL DE COMPRAS Y SERVICIOS, SL, which in turn obtained it from ATRATO MEDIA, SL and this, in turn, from BOX 24 2050 SL. A violation of article 6.1 of the GDPR is charged with a **penalty of 2,000 euros**.

There are also cases of receiving advertising via **SMS**, such as the **procedure PS/00136/2022 against AD735 DATA MEDIA ADVERTISING SL**. The origin of the procedure is a claim presented by the affected party who, after exercising their access rights, opposition and limitation of processing, you receive a commercial communication by SMS on your phone without having requested or authorized it. The violation of article 7.1 of the RGPD is punishable with a **fine of 5,000 euros**, as the person responsible for the treatment cannot prove that the data had been obtained with the consent of the claimant.

keep

Also for **obtaining personal data without consent** we find **PS/00352/2023 against SUMINISTRADOR IBÉRICO DE ENERGÍA**.

In this case, the personal data were used to formalize an electricity supply contract, without prior consent or the claimant having provided said data, proceeding to make charges to his bank account by virtue of said non-consensual contracting. A penalty of 50,000 euros is imposed for a violation of article 6.1. of the GDPR.

In the same energy sector and due to fraudulent contracting, PS/00546/2022 was resolved against IBERDROLA CLIENTES, SAU. This entity managed a change of marketer and a change of owner for a CUPS number that is not the housing number. of his client but of that of the claimant. Violation of article 5.1.d) of the RGPD is punishable with a **fine of 70,000**

**euros**.

Also for **fraudulent contracting**, we found **PS/00677/2022 against BANCO BILBAO VIZCAYA ARGENTARIA**. The origin of the file is a claim, in which the claimant revealed the theft of her bag, where her mobile phone, her ID and other documents containing personal data were located.

of that, the communication of this robbery to the bank, the impersonation of her identity and the contracting of various financial products, as well as the inclusion of the claimant in a file of defaulters. This sanctioning procedure has included issues related to this specific case and others to the established protocol, which affected the claimant and the rest of the entity's clients. **The total fine is 1,640,000 euros** for violations of articles 6.1, 32 and 25 of the

GDPR.

This sanction corresponds to **three infractions related** to the specific case reported by the claimant:

• a violation of article 6.1 of the RGPD, in relation to the **unauthorized contracting of products (70,000 euros)**,

• a violation of article 32 of the RGPD, due to the **lack of security measures** in relation to the procedures for communication, inclusion and maintenance of personal data in credit information systems (**500,000 euros**)

• and another violation of article 6.1 of the RGPD, in relation to the **incorporation of personal data in credit information systems (70,000 euros)**;

• and two other infractions related to the way in which the **protocols implemented by BBVA** were established and which were revealed through the information provided by the financial entity during the investigation actions:

- a violation of article 25 of the RGPD (500,000 euros) in relation to the protocols established for the detection of fraud

- and a violation of article 32 of the RGPD, due to the lack of security measures in relation to the procedures for contracting financial products (500,000 euros).

The sanctioning procedure **PS/00456/2022 also against BANCO BILBAO VIZCAYA ARGENTARIA**, was also initiated as a result of a claim in which the affected party indicates that, after losing her ID and filing the corresponding complaint, a third party went to a branch of the defendant impersonated her identity and was provided with banking information, in addition to giving her all of the money that was deposited in the account. Two violations of articles 6.1 and 32.1 of the GDPR are charged with **respective penalties of 50,000 and 20,000 euros**.

In the financial sector, for violation of articles 25 and 32 of the GDPR, **OPEN BANK, SA is sanctioned in procedure PS/00331/2022**, initiated by a claim submitted by an interested party to the Bavarian Data Protection Authority (Germany), because the company has not provided you with any secure means of communication to provide documentation with personal financial data.

In this case, it is concluded that OPENBANK had not foreseen the processing activity consisting of the collection of clients' financial data for the prevention of money laundering. Since this activity was not foreseen by OPENBANK, the risks to the rights and freedoms of the clients present in such treatment had not been identified and evaluated and, therefore, the appropriate technical and organizational measures have not been established or applied. to effectively apply data protection principles (including confidentiality) and comply with the requirements of the GDPR and protect the rights of data subjects (of all its clients).

All of the above shows that **OPENBANK did not comply with its obligation to apply article 25 of the GDPR, privacy by design**, neither before nor during processing. Regarding the violation of article 32 of the RGD, OPENBANK did not provide its client with an appropriate means to provide the documentation even despite the warnings of the complaining party in this regard, so the shipment was made without the necessary measures. adequate security (it did not even provide for mere encryption).

For all this, a **fine of 2,500,000** is imposed. **euros**.

In the same sector, the procedure **PS/00020/2023 against CAIXABANK** stands out, which has ended with a **fine of 5,000,000 euros** for violation of articles 5.1.f, 25 and 32 of the RGD.

This procedure was initiated due to a personal data breach in which a client of the entity has had access, for a prolonged period of time, to the receipt of a transfer made by another client and has not had proof of the update at their disposal. of data he had made. During the investigation, **flaws in the design of the computer system were detected, as well as flaws in security measures**.

Another relevant procedure regarding personal data breaches is **PS/00002/2023 against ENDESA ENERGÍA SAU** Endesa became aware of the breach due to the publication of advertisements on Facebook offering the sale of credentials to access the platform. of Endesa. After this first announcement, advertisements about the sale of credentials continued to be published on Facebook. Endesa was fined 6,100,000 euros for various infractions:

- article 5.1. f) of the RGD for **improper access to data** of millions of clients and non-clients and for not guaranteeing the integrity of the data of 760 affected people **(2,500,000 euros)**;
- article 32 of the RGD for **not having appropriate measures** before the incident and for not having taken appropriate measures after identifying the advertisements on FB **(1,500,000 euros)**;
- article 33 of the GDPR for having **notified the breach months after** detecting the ads on FB **(800,000 euros)**;
- article 34 of the GDPR for having given **information incomplete communication in the communication to those affected** (despite having been ordered by the Agency) **(800,000 euros)**
- and article 44 of the GDPR for **carrying out transfers International payments to suppliers** in Colombia and Peru **(500,000 euros)**.

Also due to **lack of adequate security measures** and other measures, **PS/00062/2022** was initiated against **AVALIA ARAGÓN SOCIEDAD DE GARANTÍA RECÍPROCA**, establishing in the resolution violations of article 5.1.f) of the RGPD (personal data is on the deep web ) and article 32 of the GDPR. **A penalty of 40,000 euros and another of 20,000 euros** respectively is imposed .

In **PS/00084/2022 against AFIANZA ASESORES**, there is also a **personal data breach** that occurred due to the theft of a USB device by an unknown person (a person external to the organization), containing documents from previous court proceedings. of the National Court, with basic, economic, contact data, and criminal infractions or convictions of 100 affected people.

Two sanctions were **imposed: 90,000 euros** for the violation of article 5.1.f) of the RGPD **and 55,000 euros** for the violation of 32 of the RGPD.

Due to **another breach of personal data**, in this case **in the health field**, in **PS/00085/2022 the HEALTH DEPARTMENT OF THE COMMUNITY OF MADRID** was sanctioned with a warning for a violation of Article 5.1.f) of the RGPD and another violation of Article 32 of the RGPD due to a confidentiality breach suffered on the web portal of the Ministry of Health of the Community of Madrid to obtain the Digital COVID Certificate. This data breach reached the press since it was possible to access the data of high-ranking figures in the State. The Ministry alleged a state of necessity and an alleged human error in the implementation of the application that allowed improper access to personal data.

In the present case, it is not possible to appreciate a state of necessity that justifies the launch of a defective or error-prone application that allows illegitimate access to personal data - including health data - of a large number of citizens, without carrying out previously carry out the necessary checks to determine its correct operation, in particular, compliance with all the obligations imposed by the RGPD and other applicable regulations.

Also in the area of **personal data breaches** in the **healthcare sector**, in this case due to a ransomware-type cyber incident,

We find **PS/00529/2022 against INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, S.L.P.**

After the investigation carried out by the AEPD, it is deduced that the measures that the clinic had were not the most appropriate, which is why violations of articles 5.1.f), 32 and 34 of the RGPD are charged, to which **a sanction of an administrative fine** would correspond. **of 50,000, 20,000 and 10,000 euros**, respectively.

Related to a **personal data breach** and due to the persistent lack of response to a request for information , **PS/00686/2022** was resolved against PREICO JURÍDICOS, SL with a **penalty of 6,000 euros**.

To put an end to the **breaches that affect personal data**, **PS / 00045/2023 against EMAILING NETWORK SARL** was initiated by the complaint of an individual in France who, when trying to unsubscribe from the clicplan.com website, only by entering the email information with which you subscribed, you were offered your personal information, without the need for a password. The French data protection authority, CNIL, carried out investigations related to EMAILING NETWORK SARL (a French company) belonging to the REWORLD MEDIA business group and found that the employees and the data protection officer of EMAILING NETWORK were in Spain. A violation of article 25 of the GDPR was declared, as an adequate risk analysis was not carried out nor measures were established to guarantee compliance with the principle of confidentiality with **a penalty of a fine of**

**10,000 euros**.

**On the other hand, cases from other EEA control authorities have increased by 51% in 2023.**



As a result of a complaint before the **data protection authority of Saxony (Germany)**, Saxon Data Protection Commissioner, **PS/00328/2022** was processed against the Spanish company THE MAIL TRACK COMPANY, SL The company offers free software for email tracking electronics so that the issuer of a

Mail is informed through the program that the recipient has opened it and when. Additionally, such emails provide a link to the mailtrack.io home page. If the recipient forwards the email, elements are inserted into the email and this could transfer your data to third parties. MAIL TRACK is accused of violating articles 13 and 14 of the RGPD, for not informing that it is responsible for the treatment (penalty of 20,000 euros); of article 6 of the RGPD, for subsequent treatments such as improving the service (penalty of 30,000 euros) and article 5.1.a) of the RGPD, for failing to comply with the principle of loyalty and transparency, given that they inform of the possibility of excluding themselves from monitoring, through a deceptive procedure (**penalty 50,000 euros**).

In **PS/00014/2023 against VACACIONES EDREAMS, SL** a claim was filed with the Hamburg data protection authority **for a right of access**. This access was denied, indicating that they should go to the corresponding telephone service to obtain access to the information. Subsequently, the representative of the complaining party insisted on receiving the response in writing, but did not receive any response to this request. A **fine of 10,000 euros** is imposed on VACACIONES EDREAMS for a violation of Article 15 of the GDPR .

Also coming from another control authority, we find **PS/00209/2022 against GLOVOAPP23, SL**. The file was initiated due to the information provided by the **Italian** data protection authority , which had carried out an investigation, in which it was discovered that The activities involved in the delivery of food or other items by delivery drivers, with the help of a specific technical platform, property of GLOVOAPP23, SL, **involved the processing of a wide range of personal data**, such as geographical location (in real time ); monitoring each step of delivery; evaluations of delivery drivers by customers or sellers; reputation scores, etc. GLOVOAPP23, SL was charged with violations of articles 13, 25 and 32 of the RGPD.

The resolution sanctions the company with a warning for violation of article 13 of the RGPD and a **fine of 550,000 euros** for violations of articles 25 and 32 of the RGPD.

Another case from another authority is **PS/00173/2023**, initiated by a claim before Urząd Ochrony Danych Osobowych, Polish data protection authority , against **YUDAYA, SL**, chain that owns the HD Acuario Lifestyle hotel (located in Las Palmas de Gran Canaria) for making a **copy of your identity document without providing you with the information required** by article 13 of the RGPD. It was resolved with the imposition of an **administrative fine of 20,000 euros** for violation of articles 13 and 15 of the RGPD.

Very similar, for making a **copy of the DNI** in a hotel establishment, **PS/00499/2022** was made against MARKETING ACCOMMODATION SOLUTIONS FZ. This company required an image of the ID on both sides to check in online and lacked a complete privacy policy. A **fine of 50,000 euros** was imposed for violating article 13 of the GDPR.

Also in the leisure sector we find **PS/00349/2022 against VACACIONES EDREAMS, SL**. The website of this company was reported for the use of the Google Analytics cookie that **transfers data to Google LLC** based in the USA after the CJEU will declare the privacy shield null and void (ruling in case C-311/18 "Schrems II"). **The cookie transfers data to Google LLC that is considered personal data**. For this reason, VACACIONES EDREAMS is considered a data exporter and Google LLC is considered an importer.

The transfers are made in breach of article 44 of the GDPR, since the privacy shield was annulled and the new adequacy decision of the Commission, dated July 10, 2023, is not automatically applicable as it requires entities to adhere to the principles. In the resolution, **no fine is imposed on VACACIONES EDREAMS, SL**, but it is ordered, for a violation of Article 44 of the RGPD, to accredit to this Agency within a period of one month that it has adapted the data processing activity. to the service of Google Analytics to the provisions of articles 44 et seq. of the RGPD, in particular by cessation of the international transfer of data until it is proven that the Google service

Analytics complies with the aforementioned provisions of the Regulation.

Another case related to **cookies** is **PS/00051/2023 against GRUPO MASSIMO DUTTI, SA** for the **use of cookies and obtaining** user consent on its website. The sanctioning procedure is processed for the commission of a violation of article 22.2 of the LSSI, due to the absence of sufficient information in the first layer about the purposes of the installation of cookies with a **penalty of 5,000 euros**.

Also for violation of article 22.2 of the LSSI, due to the **deficiencies detected on its website** regarding the "Cookie Policy", a **penalty of 5,000 euros** is imposed in **PS/00080/2023 against CHATWITH.IO WORLDWIDE, SL**, owner from the website to the website www.iurisnow.com. In this procedure, it is also confirmed that the privacy policy does not provide information about the purposes, legitimate interests and international transfers, for which a **fine of 2,000 euros** is imposed for violation of article 13 of the RGPD. It is found that there is a list of about 130 companies, of which, more than half have the "accept data processing for legitimate interest" box checked by default, which requires, in the case of wanting to show opposition to the processing, to mark the options on the list one by one, without there being the option of being able to oppose everything or reject everything. For this, a **fine of 5,000 euros** is imposed for violation of article 5.1.a) of the RGPD.

To conclude with the cases related to **cookies**, in **PS/00345/2022 against the OFFICIAL COLLEGE OF ARCHITECTS OF GRANADA**, a violation of article 22.2 of the LSSI is also sanctioned, regarding **the use of third-party cookies of a non-expected nature**, without the user's consent with **1,000 euros**. In addition, it is sanctioned for violation of article 13 of the RGPD, for the lack of information provided in the complaint forms regarding the processing of the personal data obtained, with a penalty of 8,000 euros, and for violation of article 38.6 of the RGPD, for the conflict of

interests detected in the appointment of the College Secretary as data protection delegate a **penalty of 5,000 euros**.

Also related to the figure of the **data protection delegate**, we find the procedure **PS/00253/2023 against APOLLONIA TOPCO, SL**. This **case is new** because, for the first time, the person responsible is charged with a violation of article 38.4 of the RGPD, which recognizes the right of data subjects to contact the data protection officer regarding all issues relating to the processing of their personal data and the exercise of their rights under the GDPR. The explanatory memorandum of the LOPDGDD highlights the figure of the data protection delegate that "allows the configuration of a means for the amicable resolution of claims, since the interested party may reproduce before him the claim that is not attended to by the person responsible or in charge of the treatment", which is reflected in article 37.1 of the LOPDGDD. In addition, the defendant **is sanctioned** for violation of article 5.1.c) of the RGPD, for an amount of **20,000 euros** and for violation of article 38 of the RGPD for an amount

**of 10,000 euros**.

Sanctions are also made for **deficiencies related to the data protection delegate** in **PS/00308/2023 against RAMONA FILMS, SL**

In addition to other infractions, it is alleged that **the DPD supplied** to the person complained about does not appear in the systems of this Agency and that he acted as the person responsible for some of the treatments.

On the other hand, the defendant is responsible for several web portals in which, although they have a mechanism to declare the age of who accesses the page, it does not work correctly, as it is easily circumvented, and which also does not serve to verify the age of the person accessing.

Deficiencies are also detected in signed treatment contracts and a need to adapt the privacy policy. It is resolved to impose an **administrative fine of 486,600 euros** on RAMONA FILMS, SL for violations of articles 6.1.a), 13, 28.3,32,37.38.6 of the RGPD and article 22.2 of the LSSI.



In addition to the administrative fine, it is worth highlighting the measures imposed to ensure the protection of user data, among which the establishment of appropriate security measures to adapt the age verification systems or mechanisms to the requirements stands out. legal and ensure that the personal data of minors is not processed. In the case of websites dedicated to pornography, there is a certain risk that minors will directly and without limitations access content that is harmful to them:



**The indiscriminate access of minors to pornography on the Internet constitutes a high risk to their rights and freedoms.**

In relation to this issue, the corrective measures issued in 2022 in the resolution of **PS/00555/2021 against TECHPUMP SOLUTIONS SL** have been monitored. These measures were aimed at **adapting the processing of your personal data** to the RGPD, adopting measures appropriate security measures by which the age of the users, registered or not, who access the referenced web pages is verified, guaranteeing that they are of legal age, preventing similar incidents in the future.

Several procedures related to minors have been processed. **PS /00601/2022** that begins with the transfer by the Court of Instruction No. 9, of Alicante, to the AEPD, of the proceedings followed due to the assault suffered by a minor that were dismissed as they did not constitute the facts criminal offense. **The attack was recorded by the person under investigation**, as confirmed by the Prosecutor, and for this reason they were transferred to the AEPD in case there was a violation.

A penalty of 10,000 euros is imposed **on the investigator**, who is of legal age, for violating article 6.1 of the RGPD. The measure consisting of the total suspension of all processing of personal data of minors is also adopted.

Likewise, the removal of several contents that affect minors has been required in **AI/00442/2022**.

Also related to minors, in **RR/00851/2022** the appeal presented by **FACUA against the Archive Resolution of AI/00410/2022 is dismissed**. The archive was produced because, after a procedure initiated ex officio (derived from complaints received in relation to the publication on Twitter and Facebook of some audios in relation to the Arandina case, recorded by the minor subject of abuse) and after three years During the investigations, it was not possible to determine who owned the accounts from which the audios were published (authorship could not be determined). **Reported posts containing the audio referenced in the complaints were removed** from the reported addresses.

Facua presents an appeal that was dismissed, because the complaint does not prove that the tweet was published, and the facts were already statute-barred as they dated from December 2019.

**Regarding sanctioning procedures, the area of activity with the highest number of procedures resolved in 2023 is video surveillance.**



This is the case of procedure **PS/00450/2022**, which is not an ordinary case of video surveillance, but rather involves the **installation of a video camera inside a home** rented to several tenants. Said video camera focuses on different areas of the chalet itself without a legitimizing legal basis for this treatment. It should be noted that this is the home of third parties (of the tenants) given that the "personal and domestic" scope in the capture of images of the common areas (article 22.5 LOPDGDD) disappears when the temporary use and enjoyment of the home is transferred to a third.

Going to become an area reserved for the strictest personal privacy. Due to this lack of legal basis that legitimizes the processing of the personal data of the complaining party (its image), a violation of article 6.1 of the RGPD is declared.

with a sanction of **administrative fine of 5,000 euros.**

Very similar is **PS/00496/2022 against ROMESTONE, SL** for the placement of a **video surveillance camera in the hall of a home** rented by individual rooms to students. In addition, the camera has a sound control to see if certain decibels are exceeded (in case of parties). A violation of article 6.1 of the GDPR is charged with a **fine of 6,000 euros** and the camera's removal is ordered.

Also for processing personal data of the claimants without any legitimacy contemplated in article 6.1 of the RGPD, several claims made against **QUALITY-PROVIDER SA, an entity that markets a database, have been resolved.** **PS /00030/2023**, in which a **fine of 20,000 euros is imposed**, as well as proving that they have complied with the right of deletion exercised by the claimant and adopting appropriate measures and providing the information required by the AEPD, and **PS/00517/2022**, in which a **fine of 20,000 euros is also imposed.** In this second procedure, an attempt was also made to carry out an in-person inspection, but QUALITY hindered it. This action was sanctioned in an independent sanctioning procedure, **PS/00204/2023**, in which QUALITY-PROVIDER SA is imposed, for obstruction, the investigative power that article 58.1 of the RGPD confers on the control authorities, in this case, the AEPD, a **fine of 20,000 euros.**

Related to these cases are **PS/00509/2022 against ESTUDIO INMOBILIA-RIO SAN ISIDRO, SLU** and the procedure **PS/00525/2022 against the real estate company ESTUDIO VILLALBA ANTIQUE, SL** for the **consultation of said database** without basis of legitimacy and for use the information to contact claimants. In both cases, the **fine was 5,000 euros** for violation of art. 6.1 of the GDPR.

Due to the making available of personal data without having legitimacy to do so, **PS/00058/2023 has been resolved against TECNOLOGÍA SISTEMAS Y APLICACIONES, (TECSISA).**

In this procedure, the CNMC provided a report prepared as a result of its own investigations, in which a **possible fraudulent use of the Supply Point Information System (SIPS) was observed**, indicating that a set of scenarios had been identified that suggested possible fraudulent uses of SIPS.

During the investigation, it was found that TECSISA had created the Kommodo SIPS platform, through which its clients obtained a copy of the SIPS. To access the SIPS, TECSISA used the passwords of the NCE marketer with which it had signed a data processor contract and made the information available to its clients, electricity marketers authorized and not authorized by the CNMC for access to the SIPS. SIPS data, even in a sick leave situation. TECSISA fundamentally stated that it does not access personal data. However, although it is true that according to article 7 of Royal Decree 1435/2002, marketing companies cannot access the user's identification and address data, marketing companies do access the CUPS number and this number allows identification to the owner of the supply in a univocal manner, so it is personal data.

**TECSISA is sanctioned** for violating article 6.1 of the RGPD for downloading the SIPS database without having legitimacy to do so (**penalty of 45,000 euros**) and for making authorized and non-authorized marketing companies available to the clients of the defendant. authorized to access the SIPS, the information in the database without having legitimacy to do so (**penalty of 45,000 euros**) and for the violation of article 25 of the RGPD a **penalty of 25,000 euros.**

In the telecommunications sector , procedures **PS/00266/2023 and PS/00665/2022** have been processed in which **VODAFONE ESPAÑA** is fined **100,000 euros and 140,000 euros respectively** for the **generation of duplicate SIM cards without legitimation.** The offending conduct consisted of processing personal data without legitimacy - fraudulent duplicate SIM - for not acting diligently in identifying the applicants for the duplicate.

Also for a violation of article 6.1 of the RGPD we have **PS/00271/2022 against DIGI SPAIN TELECOM**, for the **portability of the claimant's line by a third party impersonator**, with a total absence of valid measures aimed at guaranteeing the identity of the person granting consent. A **fine of 70,000 euros** was imposed .

Continuing with the telecommunications sector, in this case in relation to the exercise of rights we find the rights procedure **PD/00133/2023 against VODAFONE ESPAÑA, SAU**, in which the complaining party requested Vodafone access to a wide information, which included access to TV usage and traffic, billing and location data.

**Vodafone facilitated access to its data except for the aforementioned data on TV usage and traffic, billing and location.** Regarding TV usage data, it considers this request excessive and has justified the refusal to provide it. Regarding the traffic data necessary for billing, the resolution takes into account article 66.2 of the LGT, which provides that the operator may process them during the deadlines for challenging the bill, so nothing prevents the complaining party may have access to them during this period. Regarding the traffic and location data that are kept in compliance with Law 25/2007, as on previous occasions, it is considered that the complaining party has the right of access to such data as no limitation is established in this regard in the article 9 of the Law.

Also in relation to the right of access, **PD/00033/2023 was issued against VODAFONE ESPAÑA, SAU**. The claimant requested Vodafone access to the **geolocation data** of each of the lines contracted with said company.

Vodafone responded to this request, facilitating access to the personal data held in its systems in relation to the complainant and indicating the reasons why it was not possible to provide the history of the location and location data of all its lines. telephones.

Reasons its refusal to provide location data of the lines of ownership of the complaining party

in which Vodafone retains location and location data exclusively under the provisions of Law 25/2007, of October 18.

The resolution indicates, in relation to the interested party's right of access to the traffic and location data kept by the operators under Law 25/2007, that the operators must distinguish between the owner of the contract and the user of each line, facilitating access only to the latter.

Also with the exercise of rights, in this case of **deletion**, we find **PD/00140/2023 against ROBOTSTXT, SL** The complainant states that the durcal.net website publishes an Official Gazette of Granada in which his personal data appears. He adds that he requested the deletion of his data from the responsible ROBOTSTXT, SL and that his request was denied, citing the fact that they published on their website a copy of a public document from an official bulletin.

The claim is upheld, since the person responsible does not prove the existence of a legal basis that legitimizes the processing of the claimant's data.

**PS/00281/2022 against SECURITAS DIRECT ESPAÑA, SA** is initiated for **failure to comply with a procedure for exercising rights**, by not providing the right of access to the interested party. The access refers to the logs generated by the alarm device installed in the home of the affected person, who suffered a robbery and, according to what he states, was not notified by the Company.

SAN 3091/2019, of July 23, 2019, defines logs as "records and signals captured and sent by alarm equipment installed in a private home."

Securitas Direct does not provide all the logs to the interested party, but only those that it considers to be personal data, and with respect to these, they are supplied raw and without attaching complementary documentation for complete understanding (unawareness of the meaning of the keys that shown in the table supplied). The claimed party considers that those who

Technical logs are not personal data, among other issues because there is no influence or interaction on the part of the interested party. In addition, it alleges commercial secrecy to not provide all the logs to the interested party.

This sanctioning procedure elucidates whether the technical logs are personal data in this specific case and whether the right of access is affected by the right of commercial secret claimed otherwise.

In the resolution, it is considered that "all logs, including those generated and stored in which the owner-user does not intervene, are operated by Securitas employees in processes in which the owner does not interact, or in internal technical operations that They reveal information about the effectiveness and operation, as it is the alarm installed in your home, linked to the contract for the provision of services signed, they establish a connection between the object (the alarm) and the affected person, since the alarm is identified with a unique identifier (a specific number for each alarm device) for that service that unfaillingly links the interested party with the device and everything that is generated and recorded in relation to it.

**A fine of 50,000 euros was imposed** for violating article 58.2 of the RGPD and, in addition, measures are imposed to provide the complainant with access in the terms explained in the resolution.



**But not all procedures initiated end in sanctions. 11 % of they have been resolved with file.**

In **PS/00253/2022 against PYRAMID CONSUL-TING, SL**, during the investigation of the procedure, a **lack of accreditation was found in the facts** attributed to PYRAMID CONSULTING, regarding the incorrect identification of the complaining party as the author of an infringement of traffic, compared to the certainty and specificity required in these cases to be able to qualify the conduct

as punishable, concluding that there is insufficient evidence of charges against the aforementioned entity, which is why it was agreed to file the procedure.

Also finalized on file **were AI/00363/2022 against OIZ RIDESHARING, AI/00365/2022 against TUCYCLE BIKESHARING, AI/00362/2022 against AVANT FULLSTEP, SL, and AI/00361/2022 against ECO-LÓGICA TURISMO SOSTENIBLE, SL**

In all cases, a claim is reported in which **the communication of user data between different companies** that provide bikesharing services is reported, in which their users are not informed of such communications, and consent is not obtained. Previous investigation actions are carried out and as a result of them, it is verified that the incidents had been corrected before the claims were accepted for processing, so they are archived.

The claim in procedure **PD/00191/2023 against the Ministry of Education of Castilla y León is also rejected**. The complaining party requests the **right of access in person** to a registry of the Autonomous Administration of Castilla y León, requiring a copy of the personal data by electronic means.

The claimed party leaves it at their disposal at the secretariat of the center where the claimant is studying or alternatively at the Provincial Directorate of Education.

The debate focuses, therefore, on the means of delivery of the copy of the personal data subject to the right, since while the complaining party asserts that it has the right to have it sent by email, the claimed party indicates that The copy of the personal data is available to the complaining party, so that they can choose the one that best suits them, at the Secretariat of the educational centers, or alternatively at the Provincial Directorate of Education of León.

The regulations relate the delivery of a copy of personal data by electronic means to cases in which the interested party has exercised their right of access in this way, and without prejudice to the fact that the delivery in said format is limited to cases in which this is possible,

especially where security measures have to be applied, in particular if there are special categories of personal data involved.

Each data controller will have to determine, regarding the method of copying personal data, the means through which it will facilitate the right of access, taking into account the characteristics of its own organization, the type of personal data affected, to the precise security measures or the circumstances of the interested party, among others. And as long as it does not represent an excessive burden or impediment for the interested party (frustrating the right itself).

The **Public Administration is also the subject of investigations and procedures**, which culminate in the declaration of infringement and the imposition of measures, and which must be reported to the Ombudsman.

During 2023, several procedures have been initiated, such as **PS/00476/2022 against the Ourense City Council** for not adopting adequate measures to prevent the publication of the claimant's personal data in relation to a sentence, or to prevent the information will continue to be accessible after its removal from the website. **The City Council is sanctioned for a violation of Article 5.1.f) with a warning.**

In **PS/00031/2023, the GENERAL DIRECTORATE OF TRAFFIC is sanctioned**. In this case, the actions were initiated ex officio as a consequence of the documentation transferred by the DGT to the Legal Office for the issuance of a report on the **"Workshop Book" project**, which is a service through which car repair workshops Vehicles report to the DGT the repairs carried out on a vehicle so that the information can be consulted by any citizen, by obtaining a report on the vehicle.

It is considered that **there is no basis of legitimation since the workshops do not obtain informed, specific and free consent**. The necessary information about the purposes is not provided and there is no procedure for interested parties to withdraw consent. Nor can the treatment be protected by the public interest,

since data is collected that is not included in the regulations that regulate the Vehicle Registry and there is no rule that declares the public interest of this new processing, which constitutes a violation of article 6.1. of the GDPR. Furthermore, a risk analysis has not been carried out nor measures planned to comply with the principles of legality, accuracy and transparency, which violates article 25.1. It is also considered a violation of article 32, since workshops can access the information in the Workshop Book of the vehicles they are going to repair, but there are no measures that prevent information that is related to other vehicles and the article from being consulted. 30, since according to the DGT this new processing is integrated into the processing operations of the Vehicle Registry, but has not been included in the RAT.

Also noteworthy is the case of the **Castilla-La Mancha health service in Talavera de la Reina**, for which the sanctioning procedure **PS/00168/2022 was initiated**. The sanctioning procedure begins due to improper access to medical records by professionals from the Castilla-La Mancha **Health Service (SESCAM)**. **Warning sanctions** are imposed for violations of articles 5.1.f), 32, 33 and 35 of the RCPD. Likewise, it is proposed to the Castilla-La Mancha Health Service to initiate disciplinary actions against the people responsible for improper access and the claim is transferred to the State Attorney General's Office to analyze the possible commission of a criminal offense.

**PS /00547/2022 against the COMMUNITY OF THE REGION OF PAMPLONA** begins with following a claim filed against the Services of the Pamplona Region SA, which has implemented since autumn 2021 a system for opening waste containers through an **electronic card linked to a certain postal address**. This public company mailed an envelope in the municipality of Pamplona that contained a brochure with two electronic cards attached, as well as a sheet with "user" data and a password for a mobile application. Each card contained an address, which is that of the property whose occupant (whoever it may be, without requesting identification)

handed over the envelope. The information provided by the interested parties indicates that the container opening data, for each of the cards, is processed to analyze the use of the containers.

Although the electronic cards for opening waste containers were initially mailed, people have subsequently been able to request a new card (in cases of loss, breakdown, breakage, change of address), request the activation of the card of transport for the opening of waste containers or request credentials to activate the mobile application for opening waste containers.

In these cases, in addition to processing the personal data of the postal address, new personal data derived from the collection and registration of the presentation of the aforementioned requests have been processed: ID, name and surname, email address, telephone number, postal address, IDE transport card, signature.

The implementation of a system for opening waste containers equipped with electronic locks that correspond to Access Control Equipment (ECA) to such containers, activated by a card linked to a certain postal address, transport card activated for the opening of containers or mobile application linked to a certain postal address involves, in accordance with the definitions of article 4 of the RGPD, the processing of a set of personal data.

**The Commonwealth of the Region of Pamplona is sanctioned with a warning** for the following infractions: article 6.1 of the RGPD, articles 12.1, 13 and 14 of the RGPD, article 30.1 of the RGPD and article 35 of the RGPD.

Furthermore, the Commonwealth of the Region of Pamplona is required to, pursuant to article 58.2.f) of the RGPD, within 10 days, prove that it has ceased said processing of personal data.

On the other hand, in **RR/00027/2023** the appeal of the **Ministry of Health of the Community Board of Castilla-La Mancha** is rejected

suspension of the precautionary measure that imposes limiting or suspending the treatment imposed within the framework of **PS/00441/2021**. The Health Department of the Community Board of Castilla-La Mancha was **sanctioned** for a violation of article 35 of the RGPD.

This precautionary measure consisted of the temporary or definitive limitation of the processing of the time control system using the fingerprint, as long as it does not have a valid data protection impact assessment of the processing, which takes into account the risks to rights and freedoms of the employees and the appropriate measures and guarantees for their treatment, or even if it were carried out, it would be necessary to carry out the consultation provision established in article 36 of the RGPD.

**The appeal is dismissed and the suspension is denied** as the rights and freedoms of the officials prevail (the suspension would empty the cited part of the sanctioning resolution of its content), resulting in the fact that, in addition, they have an alternative so it is not considered that it causes serious harm to the rights of those affected and risks associated with the treatment.

Related to the **processing of biometric data** we find **PS/00553/2021 against GSMA LIMITED**. This procedure originates from a **claim by an attendee** at the Mobile Word Congress in Barcelona 2021, against the entity that organizes the Congress as the owner of the website on which the data of the attendees must be recorded. It states that to register in the "in-person" modality, you must provide a **photograph to which facial recognition techniques are applied** for security purposes.

The entity alleges that there are two modalities for registration and identification of event attendees: the so-called common system that does not involve facial recognition and the registration and identification system with facial recognition, which is based on consent.

The use of biometric data is consented by the interested parties by checking a box.

The claimant did not register in mode of use of facial recognition technology.

The procedure was initiated against GSMA LTD for the alleged violation of article 35 of the GDPR.

Although the defendant provided an Impact Assessment related to Data Protection, throughout the procedure it was considered that the impact assessment does not contain essential aspects, such as the assessment of risks and proportionality; the need for the implementation of the system, or its impact on the rights and freedoms of the interested parties and their guarantees. GSMA LIMITED **was sanctioned**, for a violation of article 35 of the GDPR, **with an administrative fine of 200,000 euros**.

Also related to the **processing of biometric data** we find **PS/00413/2022 against METROPOLITAN SPAIN, SL**. The reason for the claim that gives rise to it is that it is **required**

As a requirement for users to access their facilities, the **use of a fingerprint is required**. The system is imposed on members and anyone who does not provide their biometric data cannot access the gym. Without enabling an alternative system to make it free.

A **penalty of 27,000 euros** is imposed for violations of articles 13, 9.1 and 6.1 of the GDPR.

Furthermore, the resolution also imposes the need to accredit a correct and adequate implementation of the fingerprint use system for access to facilities, considering and accrediting its necessity and proportionality, taking into account the establishment of a lawful treatment base. for the processing of the data, also with respect to those that already have that data, and its correlative processing information associated with it, as well as proceeding to: "temporarily or definitively limit the processing" within a period of ten days on the use of the gym access system with a fingerprint, as long as it does not accommodate the legitimizing basis of the treatment and its correct information to the users.

In the **educational field**, **PS /00334/2022 was ordered against the Ministry of Defense** for the use of the Google Workspace for Education tool in the Colegio Menor Ntra. Sra.

Loreto, a private school attached to the Board of Orphans of the Navy of the Air Force, of the Ministry of Defense.

The complainant states that the school asked the parents for consent to use the tool and, although **they did not give consent**

For its use, **they registered their children in Google accounts**. A **warning penalty** is imposed for each of the violations of the RGD, articles 28 and 13.

Also in relation to the use of **Google Suite in educational centers** is **PS/00176/2022 against the Department of Education, Universities, Culture and Sports of the Government of the Canary Islands**, following the claim received against the Department of Education, Universities, des, Culture and Sports of the Government of Canary Islands-CEUCD for the use of the Google Suite application in schools.

The claimant states that the IES in which his minor son is enrolled already implemented the use of Google Suite during the 2019/2020 and 2020/2021 academic years, without requesting his consent and they registered his son despite having abandoned twisted the treatment.

The Department of Education, Universities, Culture and Sports of the Government of the Canary Islands-CEUCD **is sanctioned with a warning** for violations of articles 13, 32 and 6.1 of the RGD.

Also in the **educational field**, we can highlight **PS/00516/2022 against the Centro de Estudios Aeronáuticos SL** This file was initiated following a **claim for the request for certain data** to be able to access cabin crew training.

Among the data requested are the COVID certificate, a criminal certificate and certain data such as address, people you live with or current account number.

A **penalty of 50,000 euros** is imposed for a violation of article 9.2 of the GDPR for requesting health data and the COVID certificate and there is no circumstance that lifts the prohibition of article 9 of the GDPR; a **fine of 10,000 euros**

for a violation of article 6.1 of the RGPD for not having the legitimacy to request health data in a training course and another of **25,000 euros** for a violation of article 6.1 of the RGPD for requesting a criminal certificate and finally a fine of **5,000 euros** for a violation of article 5.1.c) of the RGPD for requesting excessive data.

Similar to this case we would also have the

**PS/00051/2022 against the Royal Federation Spanish Table Tennis** due to the **obligation to provide the COVID vaccination certificate** to enter the facilities to carry out a test.

The Federation alleged, among other things, that, to process the data, based on article 6.1 of the RGPD, it exercises a public mission since it collaborates in the training functions of technicians outlined in the Sports Law. In this case, it is not considered that he is carrying out a public action and that is why a **financial penalty** linked to the violation of article 9.2 of the RGPD with **10,000 euros** is imposed, as there is also no exception that would enable it.

Related to **health data**, in the health field there are several notable procedures.

Among them is **PS/00302/2022, in which the Health Service of the Balearic Islands is sanctioned** for a violation of article 13 of the RGPD by **not properly reporting** the bases of legitimacy of the Health Control Form (FCS). ) that travelers had to fill out when entering the Balearic Islands in August 2021 due to COVID-19.

In the resolution of the procedure, it has been considered that the obligation to comply with the principle of transparency established in article 5.1.a) of the RGPD necessarily requires that, when the treatment is based on any of the legal bases provided for in articles 6.1.c) and 6.1.e) of the RGPD (compliance

of a legal obligation or fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment) the citizen is indicated in a clear and precise manner which is the enabling legal norm regarding said treatment (in the meaning of article 8 of the LOPDGDD).

**PS /00263/2022 was filed against the Royal Spanish Handball Federation** based on a claim for the imposition of the **obligation to register the complete vaccination certificate** or, where appropriate, a negative antigen test on the Federation's platform. In order to participate in the competition, the Federation required athletes and technical staff to upload to their private area the official vaccination certificate or an antigen test with a negative result. The Federation is **sanctioned** for violating article 9 of the RGPD **with a fine of 20,000 euros**. The defendant bases the processing of health data on the circumstances contemplated in articles 9.2.d), 9.2.i) and 9.2.g), but there is no rule that includes this processing. On the other hand, none of the measures for the return to state-level competitions in the CSD protocol refer to the vaccination certificate, it only indicates that the athletes will be tested for COVID. The Federation is also sanctioned for a violation of article 13 of the RGPD **with a fine of 7,000 euros**, because, although the defendant corrected the deficiencies in the information clause during the processing of the sanctioning procedure, the clause was not complete when the data was collected in the 21/22 season, for not indicating the purpose of the processing of health data or the legal basis thereof.

The **Ministry of Education of Castilla y León was sanctioned in PS/00498/2022** for **providing** an educational center **with the complainant's vaccination data** and publishing said data on a notice board.

**Messaging applications and services** such as WhatsApp are a means by which **personal data can be disseminated improperly**, as in **PS/00270/2023 against the Sindicato Libre de Transport** or **PS/00494/2022 against Group of**



**Seguridad y Control Global, SL** In both cases, sanctions have been imposed for violating articles 5.1.f) and 32 of the RGPD, setting the **finest at 5,000 and 3,000 euros**, respectively.

For violations of the same articles of the RGPD, **PS/00452/2022 is resolved against Ilunion Seguridad SA**. In this case, a sanction is imposed for sending two emails to workers without using the hidden copy option, BCC, to the personal addresses of the workers. workers, with **finest of 10,000 and 5,000 euros**, respectively, as it is a large company.

Also in the **workplace**, **PS /00211/2023** sanctions the owner of a bar for publishing the claimant's **medical report** on her **WhatsApp status**. Given that the personal data have been exposed to third parties, a violation of article 5.1.f) of the RGPD is charged and a **fine of 2,500 euros** of the RGPD is proposed.

A violation of article 32 of the RGPD is also charged and a penalty of a fine of 500 euros.

For violation of articles 32 and 5.1.f) of the RGPD, **Pelayo Mutua de Seguros y Reaseguros a Prima Fija has been sanctioned in PS/00025/2023**.

In this case, an agent **provides a third party** with a document with the name of the insurance company that contains the **personal data** of the claimant (policyholder and insured), including her ID, insurance premium, insurance and the claims that the claimant had notified to the insurer during the validity of the contract. Violations of articles 32 and 5.1.f) of the RGPD are declared with **finest of 20,000 euros and 50,000 euros**, respectively.

In **PS/00678/2022, against Foro Asturias** for the **leak of a document** in which the claimant's payroll appears, containing his salaries and his current account number.

This claim was originally received in 2019 but was rejected due to lack of evidence regarding responsibility for the breach. However, a new claim was received in which the claimant attached a civil judgment in his favor, which declared the existence of a breach of data protection regulations by the

general secretary of a political party. In addition to the loss of confidentiality, the ruling confirms the lack of security measures that would have prevented the leak. In the resolution, violations of articles 32 and 5.1.f) of the RGPD are also declared with **finest of 5,000 euros and 15,000 euros**, respectively.

The Agency has also participated as an interested supervisory authority in various cross-border procedures within the framework of the cooperation mechanisms of Chapter VII of the GDPR.



It is worth highlighting the **procedures against large technology platforms**, established in Ireland, and therefore in which the authority of this country (the Data Protection Commission, DPC) acts as the main supervisory authority.

The first of these proceedings was directed against **Meta Ireland**, on the DPC's own initiative to examine two issues. On the one hand, if Meta Ireland acts lawfully and, in particular, in a manner compatible with Article 46(1) of the GDPR, when transferring personal data relating to persons located in the European Union or the Economic Area European Union and who visit, access, use or otherwise interact with products and services provided by Meta Ireland and, furthermore, what remedial power the DPC should apply, in accordance with Article 58(2) of the GDPR in should it be concluded that Meta Ireland is acting unlawfully and in breach of Article 46(1) of the GDPR.

The final decision adopted reflects the binding decision adopted by the European Data Protection Board (EDPB) in accordance with Article 65(2) of the GDPR, which mandates changes to some of the positions reflected in the draft Decision. of the DPC, due to the objections presented by several authorities to the draft decision, including the AEPD.

In the final decision, the DPC considers that US legislation does not offer a level of protection substantially equivalent to that provided for by EU Law and that neither the standard contractual clauses (SCC) of 2010 nor those of 2021 can compensate the inadequate protection offered by US law. Furthermore, Meta Ireland does not have complementary measures to compensate for the insufficient protection offered by US law; and cannot benefit from the exceptions provided for in Article 49, paragraph 1, of the GDPR, when carrying out data transfers.

Accordingly, **Meta Ireland considers that by carrying out data transfers, it infringes** Article 46(1) of the GDPR.

Therefore, an order is issued **requiring Meta Ireland to suspend data transfers** and to bring its processing operations into line with Chapter V of the GDPR, ending the unlawful processing, including storage, of data in the United States. personal data of EEA users transferred in violation of the GDPR. In addition, an **administrative fine of EUR 1.2 billion** is imposed in accordance with Article 58(2)(i) of the GDPR.

The second of these cross-border cases is against **TikTok Technology Limited**. The investigation in this case refers to two different sets of operations of the TikTok platform, each of which constitutes a processing of personal data. The first would be related to the **processing of personal data of minor users** in the context of the configuration of the TikTok platform. The second type of processing examined concerns the **processing of personal data of children under 13 years of age** in the context of the TikTok platform, both in mobile applications and on websites, in particular with regard to the verification of age.

Finally, with regard to the processing of personal data of minors in the context of the TikTok platform (including any such processing in relation to websites or applications that provide access

to the TikTok platform), the investigation examines whether the company has fulfilled its obligations to provide information to data subjects under Article 12(1)(e) of Article 13(2)(a) of Article 13, paragraph 2, letter b) and Article 13, paragraph 2, letter f) of the GDPR.

In the final decision adopted, the DPC declares that articles 5 (1) (c), 5 (1) (f), 24 (1), 25 (1) and 25 (2) of the GDPR have been violated in relation to the data protection by design and by default with regard to the processing of personal data of minor users.

After carefully examining the breaches identified in the investigation, the Irish authority exercised remedial powers in accordance with section 115 of the 2018 Act and article 58(2) of the GDPR, adopting:

• An order pursuant to Article 58(2)(d) for TTL to bring processing operations into compliance with the provisions of the Regulation

• A warning in accordance with Article 58(2)(b) of the GDPR; and

• Three administrative fines:

- In relation to the infringement of articles 5 (1) (c) and 25 (1) and (2), **100 million euros**.
- As regards the infringement of articles 5 (1) (f) and 25 (1), **65 million euros**.
- As regards violations of articles 12 (1) and 13 (1) (e), **180 million euros**.

In the procedure followed against **INSTAGRAM**, the complainant requests that Instagram's **consent mechanisms** be investigated, measures to prevent the illicit processing of personal data and the imposition of fines.

The draft decision issued by the DPC was objected to by several supervisory authorities, including the AEPD. Since the Irish authority did not address the objections, the case was brought to the EDPB which adopted a binding decision.

Following the Committee's binding Decision, the final decision taken by the Irish authority includes the **following corrective measures**:

☞ Meta Ireland is ordered, pursuant to Article 58(2)(d) of the GDPR, to bring the processing into compliance with the GDPR within three months from the day following the date of notification of the Decision.

☞ An **administrative fine**, pursuant to articles 58 (2) (i) and 83 of the GDPR, is imposed on Meta Ireland in the amount of **€180 million**.

Finally, proceedings were initiated against **WHATSAPP INC.**, for a claim against WhatsApp Ireland Ltd., brought by "NOYB — European Center for Digital Rights" on behalf of a German claimant. After the GDPR came into force, WhatsApp users could no longer use the service without accepting WhatsApp's terms of service. The complaint alleges that this is "**forced consent**" and that the associated data processing that users could not opt out of, in particular data processing to facilitate behavioral advertising and the improvement of services, infringed, among other things, articles 5, 6, 7 and 9 of the GDPR.

The DPC's draft decision was the subject of several relevant and motivated objections from various authorities. Since the DPC did not follow the objections, the EDPB had to rule through the binding decision.

In the final decision of the DPC, WhatsApp is ordered to adapt the processing to the Regulation within a period of six months from the day following the date of notification of the Decision and to adopt the necessary measures so that its processing of personal data for the purposes of service improvement and security measures (excluding processing for the purposes of 'IT security', as defined in paragraph 90 of the Article 65 Decision) ('the processing') is in accordance with Article 6(1) , of the GDPR. In addition, an administrative fine in the amount of EUR 5.5 million is imposed for violation of Article 6(1) of the GDPR.

These cross-border decisions can be consulted on the [website of the European Data Protection Board](#).



## ➤ 6. A resilient and constantly improving organization

### § 6.1. Talent acquisition and commitment to workplace well-being

The Spanish Data Protection Agency has a General Secretariat, which is responsible for the provision of the entity's common services, under the immediate direction of the Director of the AEPD.

In 2023, the List of Jobs (RPT) of the AEPD was subject to several expansions to adapt the workforce to the new functions to be performed by the Agency, creating a total of 41 jobs.

During 2023, four calls for free appointment were called and resolved to cover a total of 7 positions, as well as two specific competitions and two general competitions, in which 28 positions have been called (17 awarded and 11 in the process of resolution). Likewise, 16 jobs have been provided, either on secondment or provisional assignment.

Finally, in relation to the rest of the positions created, the call for applications for the appropriate selection processes is already planned in 2024.

In this sense, the AEPD is aware of the importance of attracting and retaining the best professionals, with a clear commitment to teleworking as a double instrument of work organization and conciliation, making the guarantee of service compatible with general interests. and the correct exercise of their powers, with their commitment to equality and co-responsibility, establishing specific measures for workers who have minors in their care in order to support positive motherhood and fatherhood.

With this, a high level of occupancy of the entity's positions is achieved, and the female presence at the management and pre-management levels must be highlighted. Before the approval of the AEPD Equality Plan in 2020, the Agency had 61.54% men compared to 38.46% women in these positions. As of December 31, 2023, these percentages stand at 51.45% of men compared to 48.55% of women.

**In just 4 years, the female presence at the management and pre-management levels of the Agency has increased by 10 points.**



During 2023, the Agency has vigorously resumed training actions for its staff, with special attention to those related to AEPD functions, taught by internal trainers in such specialized subjects as Tracking Technologies and Cookies, Mobile Application Analysis or Artificial Intelligence .

It is also worth highlighting the creation of a new cybersecurity area, delving into risk detection, definition of instructions, system hardening and network segmentation, internal awareness campaigns, response to incidents and vulnerability warnings, study of new solutions and adoption of those offered by the National Cryptological Center and the services of the Cybersecurity Operations Center of the General State Administration (CoCS).

## ÿ 6.2. Advance in digitalization

The AEPD continues **to advance in the digital transformation** of its processes and services to improve quality, efficiency and satisfaction in its mission.

The General Secretariat, through its Information Technology department, has completed the digitization and evolution actions of its technological infrastructure, which are described below.

In its commitment to a closer and citizen-centered administration, the Agency works to **improve the user experience** of citizens and entities, which allows them to extract maximum value from digital public services.

In this sense, the most notable aspects of the electronic office have been the following:

- ÿ Expansion of the size of the attached files that can be submitted electronically, allowing a maximum of 4 files that together reach 100 MB, instead of the 15 MB set by the electronic registration service.
- ÿ Simplification of the requirements for making a query to the Citizen Service, in its presentation through the electronic headquarters, with the enablement of the non-cryptographic signature mechanism (ie, without electronic certificate and prior authentication of the interested party through the Cl@ve platform), based on the horizontal sealing service (eUtils).
- ÿ Simplification of the presentation of candidatures to the call for the annual data protection awards, through a new specific form in the electronic office itself.

ÿ Launch of the Whistleblower Protection Channel, after the entry into force of Law 2/2023, of February 20, regulating the protection of people who report regulatory infractions and the fight against corruption.

ÿ New guided complaints mailbox, in the Advertising and commercial communication branch, to facilitate, through directed questions, the presentation of complaints with the evidence and admissibility requirements indicated in the models approved by Resolution of June 29, 2023, of the Directorate of the Spanish Data Protection Agency, by which the models for submitting claims are approved.

ÿ New functionality for the configuration and dynamic publication of alerts and news on the home page of the e-headquarters, in order to inform about technical incidents or scheduled interventions.

ÿ Automation of a first catalog of regression tests, to more efficiently and exhaustively guarantee the correct functioning of a new version of the electronic headquarters prior to its publication, and thus accelerate the availability of corrections and new functionalities.

**Web portals** are , on the other hand, the **main means of information, dissemination and first point of contact** for many people, and which then direct traffic, where appropriate, to the virtual office (or electronic headquarters) to complete communication with the AEPD, or the web assistants to help with regulatory compliance developed by the Technological Innovation Division.

In relation to these, the following can be highlighted:

ÿ Redesign of the institutional web portal, taking advantage of the technological update to the latest available version of the content management system to adapt the theme, template and

the style guide to the accessibility requirements established by the regulations and optimize it for navigation from mobile devices.

- New participation system on the institutional web portal, allowing the visitor to rate the quality of the content on a scale of one to five stars, initially in the frequently asked questions section, allowing lower scores to be accompanied by comments.
- Incorporation into the institutional web portal of a new channel for citizen service through written conversational technology (a "Chatbot"), attended by the same team that responds to telephone queries.
- Preparation of the institutional web portal to enable the language selector on all its pages, following an approach similar to that of the EDPB, in which content in different languages coexists and with integration with the automatic translation service (eTransla-tion) of the European Commission.
- Publication of the signing date in the dynamic list of claims resolutions on the institutional web portal, in response to the demand perceived from social networks.
- New functional versions of the "Asesora Brecha", "Comunica Brecha", "Evalúa Riesgo", "Gestiona RGPD" and "Valida Cripto" wizards, integrating the latter three with the content distribution network (or CDN, of the English Content Delivery Network) to improve scalability and loading speed.

In the field of **electronic processing of administrative procedures**, and with the objective of continuous technological updating, the previous application ("legacy"<sup>1</sup>) for the management of citizen service queries has been replaced by a new processing system that It additionally provides other functional capabilities aimed at improving daily management (for example, preparation and editing of documents from the application itself, etc.).

On the other hand, a new application has been developed that brings together, in a single tool, all the functions and actions necessary to carry out the **review, anonymization and publication of claims and legal reports on the institutional web portal**. The new solution therefore offers better facilities for carrying out this work, while introducing greater guarantees through controls in the publication flow and coincidence detection mechanisms.

In relation to the **management of complaints regarding data protection**, the computer processing system has continued to be improved, incorporating new functions or relevant modifications to existing ones. Progress has been made, for example, in the automation of tasks that can be performed unassisted, for greater efficiency in managing the volume of claims. Likewise, the application has a new generic search engine for files, actions and documents with greater search power, based on keywords, which at the same time offers a simpler and more usable interface. The service made available by the Data Intermediation Platform (PID) for consulting the ownership of real estate has also been integrated. On the other hand, the generation of ENI files for submission to the National Court has been reviewed, applying a new, more appropriate and intuitive organization of documentation. Finally, improvements have been made

---

<sup>1</sup> "Legacy" or inherited systems are considered those that, although supported by obsolete or outdated technologies or software, continue to be used in the organization due to their functionality and whose replacement or updating entails complexity.

in the process of composition, editing and generation of the documents that are prepared throughout the processing of a file.

As a support tool for continuous improvement in the exercise of its functions and decision-making, **the development of a long-term dashboard project has been promoted**, which facilitates the obtaining and graphical representation of the relevant indicators. for different functional and business areas.

We have continued **collaborating on initiatives with the Ministry of Justice** for the robotization and automation of processes, the use of artificial intelligence techniques in the anonymization of documents and the carrying out of procedural acts remotely.

Finally, in order to improve the quality of the software of the applications and services, throughout the year under review, substantial steps have been taken to **acquire greater maturity in the development processes**, with a first proposal of the flow continuous integration and tools applicable at each step, including test case management and automation.



**Some of these tools have already been launched and the first actions have been undertaken for their adoption in development projects.**

Internally, the Agency has continued with the **execution of initiatives for modernization and technological updating of its systems and communications infrastructure**, addressing various substantive projects, which have had as objectives homogenization, ensuring continuity, improving service and strengthening security.

Within the framework of these projects, improvements have been implemented **in the field of architecture and configuration of communications networks**; the administration and secure management of access, or server migration projects to more technologically updated and supported platforms in accordance with the CCN-STIC guides. Likewise, solutions have been incorporated that offer extensive monitoring of systems, services and applications.

Likewise, the **focus has been on improving the technical means for adequate in-person attention**, the ubiquity of the workplace and, in general, the provision of support and customer service. For example, regarding a new ITSM2 service management solution, the definition and programming of a catalog of incidents and typical requests, flows and automations has been undertaken that, adjusted to the needs of the Agency, seek to achieve greater efficiency. and agility in resolving service requests.

Likewise, throughout the year covered by this Report, a **special effort has been made in the audiovisual support for the celebration and broadcast of live events**, with improved equipment, to bring its content closer to any interested person.

On the other hand, in the field of **cybersecurity**, a new specific area dedicated to this purpose has been established, which has made it possible to delve deeper into the detection of risks, definition of instructions, or preventive actions against possible incidents or vulnerabilities and, in general, with the purpose of improving the security of systems and services.

In this sense, the development of a **Risk Treatment Plan** aimed at compliance with the ENS3 measures has been addressed. Likewise, various prevention and detection services made available by the Center have been adopted.

<sup>2</sup> ITSM: IT Service Management, or Information Technology service management.

<sup>3</sup> ENS, or National Security Scheme, defined by Royal Decree 311/2022, of May 3, which regulates the National Security Scheme.

National Cryptology (CCN) and the Cybersecurity Operations Center of the AGE (COCS). And implemented the policy established by the General Secretariat of Digital Administration (SGAD) for the security of mobile devices.

Likewise, progress has continued, with greater momentum, in the application of **measures for perimeter protection**, as well as the bastion of devices and systems.

Finally, aimed at staff, a **cybersecurity training and awareness program** has been launched that, divided into modules and short practical exercises, employees can complete at their own pace and interactively.

### 6.3. Efficiency in resource management

The economic and financial management of a public body such as the AEPD requires planning and correct administration of the organization's resources.



**In 2023, the AEPD's initial expenditure budget has amounted to 18,750,730 euros, 11.1% higher than in 2022, to meet the needs of creating new jobs to adapt the staff structure to the functions of the Agency.**

As in previous years, **the level of budget execution has remained high**, above 90%, specifically, at 93.2% for the year 2023. The remainder has occurred mainly in chapter 1 "Personnel Expenses", due to the gap between the creation of the positions and their coverage after the corresponding selective processes.

With regard to the execution of its income budget, as of December 31, 2023, **the amount of gross rights recognized has amounted to 31,778,046.02 euros**, of which 95.3% (30,278,978.16 euros) correspond to rights recognized by sanctions. For its part, **the amount of net recognized rights stood at 30,110,633.52 euros**, once the insolvencies or cancellations that occurred during the year were taken into account.

The **total collection** in the current fiscal year 2023 amounts to **15,234,956.45 euros**, of which 13,735,888.59 euros correspond to sanctions (90.1%).

The **net collection of sanctions**, in the current fiscal year 2023, has been **13,656,315.03 euros**, once the refunds of sanctions have been accounted for.

Taking into account the collection of recognized rights from years closed during the current year, the total collection of sanctions in the fiscal year 2023 has been 14,868,210.64 euros, and the total net collection of sanctions has been 14,788,637.08 euros, once the returns of income as a result of the partial or total estimation of resources have been accounted for.

Finally, as a novelty during 2023, **it should be noted that the amounts deposited** in the current accounts opened in the name of the AEPD **have generated financial income in the amount of 1,452,202.24 euros.**



## 7. The necessary institutional cooperation

### 7.1. consultive advice

The Agency's Advisory Council, the collegiate advisory body of the Directorate, met in 2023, on two occasions.

At the meeting on July 11, the great increase in activity of the AEPD in all its subdirectorates and divisions was revealed, **highlighting the significant increase in the number and complexity of complaints received, 33.3% compared to the previous year. same semester of the previous year**; as well as the steps taken by the Agency to protect the privacy of minors on the Internet, an initiative valued very positively by the members of the Council.

At the meeting on December 11, in addition to presenting the activity of the different units, the winning works in the call for the 2023 AEPD awards **were designated** .

Both meetings were held in a mixed format, combining the presence of some of its members and facilitating the telematic intervention of those who did not travel to our headquarters, taking advantage of the facilities introduced in Law 40/2015, of October 1, of the Legal Regime of the Public Sector, which provide for the possibility that the sessions be held remotely, the calls be sent by electronic means and that the sessions can be recorded.

### 7.2. Autonomous authorities

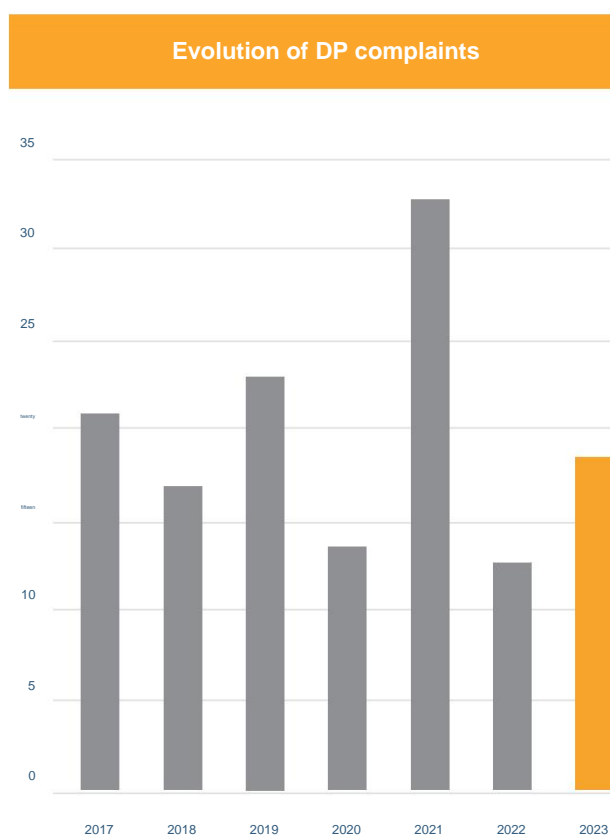
In May 2023, a meeting was held with the participation of the Spanish Data Protection Agency, the Catalan Data Protection Authority, the Basque Data Protection Agency and the Transparency and Data Protection Council of Andalusia. in which topics related to the data protection implications of ChatGPT were discussed, the implications of Law 2/2023, of February 20, regulating the protection of people who report regulatory infractions and the fight against corruption from the point of view of data protection regulations, the procedure for the declaration of warnings after the LOPDGDD reform, initiatives for evaluating the impact on data protection in the regulatory process, practical experience from the control authorities after receiving notifications of a security breach, the guidelines on cookies and web analytics on public administration portals, the preliminary guidelines for the implementation of data protection from the design in the Data Space.

Likewise, information was provided on the AEPD's circular of article 66.1.b) of the LGT regarding the legal regime of telephone advertising and on the activities of the European Data Protection Committee.

Finally, opinions were exchanged on the working group meetings of the Data Protection Authorities.

## 7.3. Relations with the Defender from town

During the current year 2023, **a total of 18 matters have been processed**, compared to 12 last year.



Regarding the **reasons** that have led citizens to contact the AEPD through this channel, the main one, on seven occasions, has been related to **the complaint about the lack of response within the deadline for the resolution of the corresponding claims or requests for information made to the Agency**. Along with the already mentioned requests for information on the measures adopted by public administrations in compliance with the Agency's resolutions, **the request for information on the measures adopted stands out**.

In one case, the Ombudsman's request for information on the reasons that justify the transfer of data by the

General Directorate of the Police and the General Directorate of Internal Policy to the General Treasury of Social Security.

And by the General Directorate of Internal Policy to the Police, indicating the date of submission of the same.

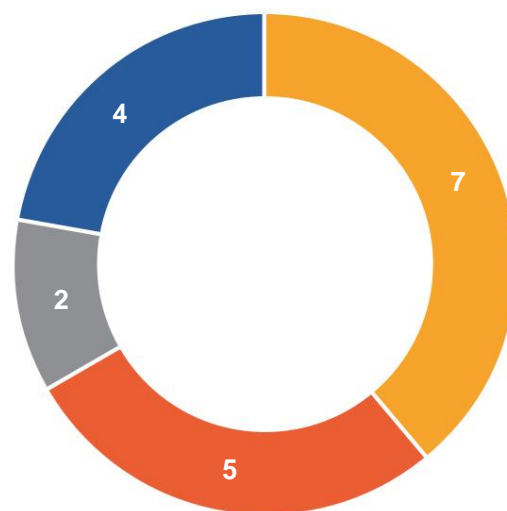
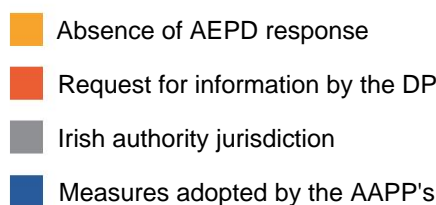
In two cases, information has been requested about claims for which, within the framework of Regulation (EU) 2016/679, General Data Protection, the AEPD was not the competent authority for processing, having been sent to the authority of Protection of Ireland, as the main authority, a circumstance notified to the complainants in both cases.

Finally, in one case a reminder has been received from the Ombudsman regarding compliance with the legal duties of timely resolution of claims and appeals presented to the Agency.

This letter was responded to by arguing in detail about the Agency's workload due to the exponential growth in the number of claims presented, the complexity and increase of the cross-border procedures in which it has intervened, and the legal and technological qualification requirements of the claims raised that, additionally, affect the qualification of the professionals who join the Agency, making a period of adaptation necessary, and reporting on how these circumstances have been revealed in the appearances of the Director in Congress of the Deputies.

The writing ends by referring to the technological measures aimed at achieving greater automation of the procedures that allow their simplification and streamlining, as well as the Agency's initiatives for the modification of Organic Law 3/2018, of December 5, of Protection of Personal Data and guarantee of digital rights, which have been processed to obtain greater efficiency and effectiveness, in particular, promoting mediation procedures for the processing of claims in accordance with the provisions of the General Data Protection Regulation (GDPR).

## Reasons for complaint



## 8. An active authority on the international scene

### 8.1 European Union

#### 8.1.1 European Data Protection Committee (CEPD)

The activity of the European Data Protection Committee has been intense throughout 2023. The Agency has participated very actively in these works. The Agency is represented in all the expert subgroups of the European Committee and acts as coordinator of one of its subgroups, the so-called Compliance, Health and eGovernment subgroup (“Compliance, Health and eGovernment”).

In order to fulfill its mission of ensuring the consistent application of the GDPR throughout the European Union, the EDPB has continued its work on developing and approving Guidelines that clarify and provide guidance on different aspects of the application of the Regulation. **During the year 2023 CEPD has approved the following Guidelines:**



Finally, the AEPD has participated as **main editor or co-editor** in several of the documents that the Committee has published in 2023.

**Guidelines 2/2023: On the technical scope of Art. 5(3) of the Directive on privacy and electronic communications (Directive 2002/58/EC, ePrivacy)**

The objective of these guidelines is to carry out a technical analysis on the scope of application of article 5 section 3 of the European Directive

on privacy and electronic communications. Specifically, they aim to clarify what is meant by storage or access to information stored on the terminal equipment of a subscriber or user. The guidelines do not address the circumstances under which a processing operation may fall within the exceptions to the consent requirement provided for by the Directive.

The emergence of new tracking methods to replace existing tracking tools (e.g. cookies, due to the discontinuation of support for third-party cookies) and the creation of new business models has become a critical concern in the field of data protection. While the applicability of Article 5(3) of the ePrivacy Directive is clearly established for some tracking technologies, such as cookies, it is necessary to remove ambiguities related to the application of this provision to tracking tools. Emerging technologies, such as tracking pixels and URLs, IP address-based tracking, local processing, and unique identifiers, among others.

These **guidelines 2/2023** have been submitted to public consultation in the version available in the following [link](#). The final version is pending publication.

#### **Guidelines 1/2023: Regarding article 37 of the Police directive (680/2016)**

They provide additional guarantees for International Transfers in matters of police and judicial cooperation to third states in the absence of a decision from the European Commission. In this agreement has been reached **on two points:**

**to.** In the case of art. 37 a) that allows the controller to evaluate the specific guarantees to be implemented for a specific transfer, the guides suggest that it is preferable to avoid this evaluation and for the controller to resort to the transfer tools of title V of the RGPD.

**b.** In the event that the controller evaluates the guarantees that the transfer already incorporates in a legally binding instrument are adequate, it must consider the risk to the fundamental rights of the affected party in view of the data protection of the third State in question and weigh the legitimate interest of other people who may be affected.

These **guidelines 1/2023** have been submitted to public consultation in the version available at the [following link](#), pending approval and publication for the final version.

#### **Guidelines 9/2022: On notifications of security breaches under the GDPR**

Due to certain doubts regarding security breach notifications, the EDPB decided to modify the Guidelines published by the former Article 29 Working Group. The modification is limited to paragraph 73 and clarifies that the mere presence in any European Union country of a representative of a controller who is outside the Union does not mean that the single window system can automatically be used. In these cases, security breaches must be notified to all affected data protection authorities.

These **9/2022 guidelines** were submitted to public consultation after which they were approved in their final version available at the [following link](#).

#### **Guidelines 8/2022: On the identification of the main authority for a person responsible or in charge**

The guidelines aim to clarify the concept of main establishment in the context of joint controllers taking into account the European Data Protection Board Guidelines 7/2020 on the concept of controller and processor.

The guidelines address the concepts of cross-border processing, providing criteria for carrying out a test to determine whether said processing “substantially affects”, according to the definition of cross-border processing included in Article 4 of the GDPR, data subjects in more than one Member State. and analyze the concept of main establishment.

Based on the previous concepts, a procedure is provided to identify the main supervisory authority in different scenarios: main establishment other than the location of the administrative headquarters in the European Economic Area, group of companies, joint controllers, other borderline cases, etc., providing examples in each scenario for a better understanding.

These **8/2022 guidelines** were submitted to public consultation after which they were approved in their final version available at the [following link](#).

#### **Guidelines 7/2022: On certification as a tool for international transfers**

The GDPR requires in article 46 that data exporters establish adequate guarantees for transfers of personal data to third countries or international organizations.

Among the appropriate guarantees provided for in article 46 of the GDPR is certification, as developed in article 42.

These guidelines provide guidance on how certification should be used to provide the appropriate guarantees required in international transfers.

To this end, the guidelines are structured into four sections that address, among others, the certification process, the accreditation of certification bodies, the assessment criteria of the regulations of the importing country, the general obligations of exporters and importers, the rules for onward transfers, redress and enforcement mechanisms, actions for situations where legislation

and national practices prevent compliance with the commitments assumed as part of the certification and requests for access to data by third country authorities, binding commitments between those responsible and processors not subject to the GDPR but adhered to certified by contract or other binding instrument to comply with the appropriate safeguards provided by the certification mechanism.

In addition to the aforementioned four sections, an annex is included with examples of supplementary measures in line with those included in Annex II of Recommendations 01/2020, on measures that complement the transfer tools to guarantee compliance with the level of protection. of EU personal data.

These **guidelines 7/2022** were submitted to public consultation after which they were approved in their final version available at the [following link](#).

#### **Guidelines 5/2022: On the use of facial recognition technologies in the police field**

The objective of these guidelines is to provide a series of guidelines to align facial recognition processing in the field of police cooperation with the GDPR.

The guide points out that police and judicial authorities are increasingly using facial recognition technologies to identify people from photographs or videos for different purposes and with the support of other additional technologies such as artificial intelligence, machine learning or “big data”.

Among the purposes are the processing of lists of suspects or the monitoring of people's movements in public spaces. These large-scale treatments can affect fundamental rights such as the right to privacy and produce discrimination and even false results.

The guide establishes that any limitation on the exercise of fundamental rights and freedoms must have a legal basis and respect the essence of those rights and freedoms. The legal basis must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances under which the authorities are empowered to resort to any data collection and secret surveillance measures, therefore, In the opinion of the European Data Protection Board, a mere transposition into national law of the general clause contained in Article 10 of Directive (EU) 2016/680 (LED Directive) would not be valid as it lacks the necessary precision and predictability in the limitation of fundamental rights and freedoms.

The guide advocates a prohibition on the use of these technologies in public spaces and advocates respect for the principles of purpose and proportionality of data processing in their use. Furthermore, the legislative measures intended to implement its use must be appropriate to achieve the legitimate objectives pursued by the legislation in question. An objective of general interest, no matter how fundamental, cannot in itself justify a limitation on a fundamental right. Legislative measures must differentiate and identify those targeted in light of the specific objective, for example, the fight against specific serious crimes.

These **guidelines 5/2022** were submitted to public consultation after which they were approved in their final version available at the [following link](#).

#### **Guidelines 4/2022: On the calculation of administrative fines under the GDPR**

The objective of these guidelines is to provide a series of guidelines to GDPR supervisory authorities for calculating the amount of fines related to violations of the GDPR, with the aim of harmonizing these amounts.

These guidelines complement previous guidelines of the Committee (on the application and establishment of administrative fines in the Regulation, WP253, endorsed by the Plenary of 25 May 2018) and whose practical application had revealed its shortcomings.

The new guidelines, in addition to harmonizing the methodology to be followed for calculating the amounts of fines, aim to increase clarity and transparency in this type of operations, as well as guarantee the application and compliance of the Regulation.

This document specifies the provisions of article 83 of the Regulation, which establishes a series of general conditions for the imposition of fines. Among other things, this article provides that each authority will ensure that fines are effective, proportionate and dissuasive.

It also establishes a series of criteria to be taken into account by the control authorities when deciding the imposition of fines and their amount in each individual case.

In any case, it is necessary to always keep in mind that the general rules contained in these guidelines are understood without prejudice to the specific and concrete circumstances of each file.

These **4/2022 guidelines** were submitted to public consultation after which they were approved in their final version available at the [following link](#).

#### **Guidelines 3/2022: On misleading patterns on social media interfaces: how to recognize and avoid them**

The aim of these guidelines is to provide practical recommendations to designers and users of social media platforms on how to evaluate and avoid so-called "deceptive patterns" in social media interfaces that violate the requirements of the GDPR.

The document includes a list of deceptive patterns and best practices, as well as use cases, although this list is not exhaustive.

Social media providers remain responsible for ensuring their platforms' GDPR compliance.

These **guidelines 3/2022** were submitted to public consultation after which they were approved in their final version available at the [following link](#).

### **Guidelines 1/2022: On the rights of those affected – the right of access**

With the aim of creating guidelines on the rights of the affected person under the GDPR, we have started with the right of access addressed in these guidelines.

The general objective of the right of access is to provide people with sufficient, transparent and easily accessible information about the processing of their personal data so that they can know and verify the legality of the processing and the accuracy of the data processed. This makes it easier for the affected party to exercise other rights such as deletion or rectification, although the exercise of the right of access is not a prerequisite for the exercise of other rights.

The guidelines address aspects such as the no need for justification by the interested party when exercising this right, the scope of the exercise of this right especially when it affects the rights of third parties, the additional information that the response to the right must contain. of access apart from the personal data of the interested party, as well as the format and means by which the person responsible for the treatment must provide the right with special consideration when the volume of information to be provided is large.

The guidelines also address cases in which the controller may refuse the exercise of the right, as well as those cases in which the controller may demand

the payment of the cost of said exercise, taking into account that, as a general rule, the right must be free of charge.

These **guidelines 1/2022** were submitted to public consultation after which they were approved in their final version available at the [following link](#).

### **Guidelines 5/2021: On the relationship between the application of article 3 and the provisions on international transfers of the GDPR Chapter V**

These guidelines are a consequence of those previously adopted on the territorial scope of the GDPR (Guidelines 3/2018).

In the process of preparing those guidelines, the question was raised about the consideration that should be given to data communications from processors located in the EU and controllers not established in it when these communications occurred within the framework of data processing. subject to the RGPD by virtue of its article 3.2.

Several delegations maintained that, to the extent that the data leaves the EU, there would be an international transfer, while, for others, the fact that the data did not leave the scope of protection of the GDPR meant that it could not be referred to as an international transfer.

This doubt, together with the fact that the GDPR does not contain a definition of what should be understood by "international data transfer", has led to the preparation of these present guidelines.

For the Committee, **an international transfer exists when the following three requirements are met:**

- The controller or processor (exporter) is subject to the GDPR for the processing in question.
- The exporter communicates by sending or by any other means that the personal data, subject to this processing,

They may be made available to any other person responsible, jointly responsible or in charge (importer).

- The importer is located in a third country or in an International Organization, regardless of whether or not the GDPR applies to the importer with respect to the processing in question in accordance with art.3 of the GDPR.
- As can be seen, this definition of transfer already includes the response to the controversy regarding the application or not of the concept of international transfer for treatments subject to the RGPD by virtue of art. 3.2, since, according to the third of the requirements, the fact that the importer is in a third country determines the existence of a transfer regardless of the regime to which the treatment in which it is framed is subject.

Other **elements of interest** in the guidelines are:

- A transfer is not considered in the event that a controller in a third country collects personal data directly from a data subject in the EU, since there is no "exporter".
- A transfer is not considered in the event that an employee of a controller in the EU travels to a third country for professional reasons and accesses the data contained in the controller's records, given that there would be no "importer" other than the controller himself to which the employee works.

These **5/2021 guidelines** were submitted to public consultation after which they were approved in their final version available at the [following link](#).

#### **Guidelines 3/2021: On the application of article 65.1.a of the GDPR**

Chapter VII of the GDPR includes the mechanisms of cooperation and coherence between the supervisory authorities that apply to cases of cross-border processing. Article 60 establishes the procedure to be followed for the resolution of said cases, through a final decision that must be unanimously agreed upon by all the control authorities participating in the case. When unanimity is not possible, the GDPR provides for the coherence mechanism established in article 65.1.a), which grants the EDPB the ability to issue a decision that is binding on all supervisory authorities participating in the case.

In order to establish a procedure for this conflict resolution mechanism, the Committee has developed guidelines that establish certain concepts and identify the steps to follow when applying this procedure.

These guidelines are closely related both to those being developed on the cooperation mechanism of article 60 GDPR, which are referred to later, and to those approved in 2020 on the notion of Relevant and Reasoned Objection.

Among the criteria established in the guidelines on article 65, the sections on the limits and contents of the decisions that the Committee can adopt and on the implementation of the "right to be heard" before the Committee for interested parties are especially noteworthy. -sadas that may be affected by the decision of the Committee

These **3/2021 guidelines** were submitted to public consultation after which they were approved in their final version available at the [following link](#).



## OPINIONS

### Opinion 5/2023, on the proposal for a decision on the adequacy of the EU-US privacy framework (DPF)

On December 13, 2022, the European Commission published a draft Adequacy Decision on the new scheme agreed with the US government for transatlantic exchanges of personal data called the EU-US Data Privacy Framework. (DPF, for its acronym in English), which aims to replace the previous scheme called Privacy Shield or Privacy Shield invalidated by the Court of Justice of the European Union (CJEU) on July 16, 2020, in the Schrems II case .

In accordance with article 70.1.s of the GDPR, the Commission requested the opinion of the European Data Protection Board (EDPB) on the draft Decision.

In its opinion, the EDPB evaluated the adequacy of the level of protection granted in the USA, based on the examination of the draft Decision, covering both commercial aspects and access and use of personal data transferred from the EU by the public authorities of the United States.

To this end, the EDPB took into account the applicable EU legal framework on data protection established in the GDPR, as well as the fundamental rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter. of the Fundamental Rights of the European Union and in article 8 of the European Convention on Human Rights. It also examined the application of the right to an effective defense and a fair trial established in Article 47 of the Charter, as well as the jurisprudence of the CJEU on the protection of fundamental rights.

Finally, the CEPD approved, on February 28, 2023, its opinion 5/2023. For its part, the European Commission, after collecting part of the

recommendations contained in the previous opinion, adopted, on July 10, 2023, the decision to adapt the new EU-US privacy framework. This framework will be periodically monitored by the Commission in collaboration with the EDPB.

This CEPD **opinion 5/2023** is available at the [following link](#).

### Joint opinion EDPB-EDPS 1/2023, on the proposed Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the implementation of the GDPR

On 07/04/23, the European Commission (EC) published a proposal for a Regulation to establish additional procedural rules related to the implementation of the GDPR and limited to cross-border processing. This proposal aims to agree on rules for the processing of complaints, as well as for carrying out investigations by supervisory authorities.

Jointly, the EDPB, together with the European Data Protection Supervisor (EDPS), approved this opinion in which both organizations favorably welcome the Commission's proposal, aimed at strengthening effective compliance with the provisions of the GDPR. They also point out that its early adoption is of capital importance to continue improving the efficiency and consistency of the GDPR.

This joint opinion is therefore a reference to be taken into account in the negotiations that are taking place to approve this new Regulation, since it has been adopted by the competent bodies in matters of data protection within the EU. .

This joint **EDPB-EDPS opinion 1/2023** is available at the [following link](#).

### Joint opinion EDPB-EDPS 2/2023, on the proposed Regulation of the European Parliament and of the Council for the establishment of the digital euro

The European Central Bank (ECB) published a report on the digital euro on October 20, 2020, the possible issuance of which is the exclusive prerogative of the ECB. Subsequently, on 28 June 2023, the European Commission proposed a legislative package on a digital euro, including a proposal establishing the legal framework for a possible digital euro, and formally consulted the EDPS and the EDPB in order to issue a joint opinion on said proposal.

The EDPB and the EDPS rate certain aspects of the proposal very positively, such as that users always have the option of paying in digital euros or in cash, that the digital euro is not "programmable money" and that the proposal aims provide a high level of privacy and data protection for the digital euro and, in particular, by introducing an "offline mode", to minimize the processing of personal data in relation to the digital euro, as well as to integrate data protection by design and by default.

However, the EDPB and EDPS draw the attention of co-legislators to a number of potential risks to the protection of personal data which, if not addressed in the proposal, could undermine citizens' confidence in the future digital euro and, ultimately, its social acceptance. Possible risks include those related to the establishment of unique identifiers, the mechanisms for detecting fraud, the pseudonymization of transactions between the ECB and national central banks, the applicable legal bases and the categories of personal data that must be processed by the different agents involved, the relationship with the fight against money laundering and the financing of terrorism, among others.

This **joint EDPB-EDPS opinion 2/2023** is available at the [following link](#).

### Opinions on Corporate Rules Binding (BCR)

The GDPR provides in its article 46.1 that, in the absence of an adequacy decision according to article 45.3 of the GDPR, a controller or processor may transfer personal data to third countries or international organizations only if the controller or processor has provided adequate guarantees and on condition that the interested parties have enforceable rights and effective legal actions.

A group of companies engaged in a joint economic activity can provide such guarantees through the use of legally binding BCRs, which expressly confer enforceable rights on the data subjects and meet a number of requirements (Article 46 of the GDPR).

The implementation and adoption of BCR by a group of companies aims to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country.

The BCRs are subject to the approval of the competent supervisory authority, in accordance with the consistency mechanism established in articles 63 and 64.1 of the RGPD, which must verify that said BCRs satisfy the conditions established in article 47, together with the criteria established by the CEPD in the guidelines established for this purpose WP256 rev.01 of GT 29 and adopted by the CEPD)

During the year 2023, a total of twenty-seven BCRs presented by the following countries received a favorable opinion: Holland, Denmark, Germany, France, Romania, Belgium, Ireland, Spain and Italy.

These documents on **Binding Corporate Rules** can be accessed at the [link](#).

### Opinions on the accreditation requirements of code of conduct supervisory bodies and certification entities

The GDPR establishes that codes of conduct must have a supervisory body that monitors compliance with the code by those responsible for it. This body must be accredited by the national authority following accreditation requirements, which must be presented to the CEPD for approval. During 2023, a total of four accreditation requirements were submitted by the authorities of Sweden, Croatia, Romania and Latvia, which have received a favorable opinion.

Similarly, before approving a certification mechanism in accordance with art. 42 of the GDPR, it is necessary to establish the accreditation requirements of the certification entities that will be dedicated to issuing the certificates.

These requirements can be developed by the authority itself or, if the body in charge of accreditation is the national accreditation body (NAB), additional requirements must be established to the ISO 17065 standard. In any case, the requirements must be approved by the CEPD by means of an opinion. During 2023, a total of five accreditation requirements were submitted by the authorities of Slovenia, Luxembourg, Croatia, Cyprus and Malta, which received a favorable opinion.

You can **access these documents** through the [link](#).

### Opinions on certification schemes

The GDPR provides that some treatments may be subject to certification to help demonstrate that they are carried out safely and in compliance with the fundamental right to data protection.

Entities can develop certification schemes that are subject to the scrutiny and approval of the CEPD.

During the year 2023, opinion 15/2023 was approved on the certification criteria called "Brand Compliance certification standard", presented by the entity Brand Compliance BV through the Dutch authority, and which received a favorable opinion. These **certification criteria** are intended to ensure consistent application of the GDPR except for international transfers.

You can **access these opinions** on certification schemes through the [link](#).

## RECOMMENDATIONS

### Recommendations 1/2022 on the Approval Request and on the elements and principles found in the Binding Corporate Rules of the Controller (BCR) (Art. 47 GDPR)

Their objective is to clarify the requirements that the BCR must meet in relation to the obligations of those responsible and in charge of the BCR (BCR-C and BCR-P) in order to guarantee the same conditions of equality for all applicants from BCR.

The recommendations have been made in order to update previous recommendations on BCR contained in documents WP 256 rev.01 for BCR-C, and WP 257 rev.01 for BCR-P, as well as to include the standardized application forms that must be used by the BCR requesters and contained in Article 29 Working Group document WP264 for BCR-C and WP265 for BCR-P, respectively.

The recommendation also incorporates the requirements indicated by the CJEU in its Schrems II Ruling, in relation to the main elements contained in the new Standard Contractual Clauses of the European Commission to carry out international transfers of personal data to third countries. Furthermore, these recommendations incorporate the experience accumulated by data protection authorities in the course of approval procedures for specific BCR requests since the entry into force of the GDPR. **The approval of the BCR is a task that must be carried out by all the Supervisory Authorities members of the EDPB working in the same way**, and therefore it is very important to reach a common understanding, among all the Supervisory Authorities, on the requirements that must be included in the BCR and on your application form.

After being submitted to public consultation, **the recommendations** were approved and are available at the following [link](#).

## BINDING DECISIONS

Under Article 65 of the GDPR, the EDPB has the power to adopt binding decisions when no unanimous agreement is reached between the lead authorities and the interested parties on proposed decisions in cross-border cases. **This is the so-called dispute resolution mechanism.** In 2023, the EDPB has adopted two binding decisions relating to Article 65 of the GDPR as well as one urgent binding decision relating to Article 66 of the GDPR, which are detailed below:

### Binding Decision 1/2023 on the litigation brought by the Irish Supervisory Authority regarding data transfers made by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR)

In the present case, the main supervisory authority was that of Ireland (Data Protection Commission - DPC) and the person responsible for the processing investigated was META Platforms Ireland Limited (formerly Facebook Ireland Limited).

This case revolves around the legality of the transfers that this person responsible has been making to META US. These were systematic, massive, repetitive and constant (that is, not occasional or sporadic).

In its draft decision of 07/06/22, DPC considered that this person committed a violation of article 46.1 of the Regulation. That authority ordered the suspension of transfers to that country, on the basis that American legislation did not provide a level of protection equivalent to that of the European Union/ European Economic Area.

The resolution of the dispute revolved around the need to impose two additional coercive measures for having committed this violation.

On the one hand, a fine that must be effective, proportional and dissuasive. On the other hand, and with

In relation to the data already transferred to the USA, an order to META to comply with Chapter V of the Regulation, and the illicit processing of these data in that country must cease (including its conservation). The Committee's binding decision included both additional measures.

This **binding decision 1/2023** can be consulted at the [following link](#).

**Binding decision 2/2023 on the litigation brought by the Irish Supervisory Authority regarding TikTok Technology Limited (Art. 65 GDPR)**

In the present case, the main supervisory authority was that of Ireland (Data Protection Commission - DPC) and the person responsible for the processing investigated was TikTok Technology Limited (TTL).

This case mainly revolves around the effectiveness of the technical and organizational age verification measures adopted by TTL during the reference period (from 07/31/20 to 12/31/20), as well as on a possible additional violation of the principle of loyalty.

The EDPB decided that it does not have enough information in this case to conclusively assess TTL's compliance with article 25.1 GDPR (data protection by design), despite its serious doubts about the effectiveness of these measures. The CEPD admitted the additional violation of the principle of loyalty, and ordered DPC to take it into account in its final decision. The EDPB ordered that the final Irish decision include the removal of the deceptive design patterns identified in this binding decision, within a timeframe determined by DPC.

This **binding decision 2/2023** can be consulted at the [following link](#).

**Urgent Binding Decision 01/2023 requested by Norwegian Supervisory Authority to order definitive measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)**

The Plenary of the Committee adopted on 10/27/23 the urgent binding decision (UBD) 01/2023, on FACEBOOK and INSTAGRAM. The Norwegian Supervisory Authority was the one who requested this decision, in application of article 66 of the GDPR. META Ireland (META) is responsible for the processing in question, with the main authority in the case being that of Ireland (DPC) and the rest of the authorities of the European Economic Area interested in the

case.

Norway brought this case because CEDP binding decisions 03/2022 (on FACEBOOK) and 04/2022 (on INSTAGRAM), both dated 12/05/22, told DPC that META improperly relied on Article 6.1.b ) GDPR to process a complainant's data to carry out behavioral advertising (BA), and that it did not rely on any other legal basis to carry out BA, so it lacked a legitimizing legal basis for process those data for that purpose, therefore violating article 6.1, which is why it had to receive a compliance order from DPC to comply with that provision within a period of 3 months.

In application of these binding decisions, DPC adopted its resolutions IN-18-5-5 (on FACEBOOK) and IN-18-5-7 (on INSTAGRAM) on 12/31/22, which reproduced what was previously stated by the Committee.

The Plenary of the CEPD on 10/27/23 ordered DPC to order the prohibition of carrying out BA by META, based on 6.1.b) and 6.1.f) GDPR. It took into account that, more than 6 months after the expiration of the period that META had to adapt to this provision, that person in charge was still not complying with this article.

This **binding decision 01/2023** can be consulted at the [following link](#).

## REPORTS

### EDPB contribution to the report on the implementation of the GDPR according to Article 97

Under Article 97 of the GDPR, the Commission must present a public report to the European Parliament and the Council in 2024 evaluating its implementation.

At its December plenary session, the EDPB adopted this contribution so that it can be taken into account by the Commission in the aforementioned report.

In its report, the CEPD estimates that, only five and a half years after the entry into force of the GDPR, it is premature to open its review process, considering that it is advisable to wait until we have more elements that allow us to appreciate the aspects that this important regulation Needs improvement. Once more perspective is available, that process can be launched.

The EDPB calls on European legislators and the Commission to work towards greater clarity and homogeneity regarding the new functions and powers of supervisory authorities. It also asks them to guarantee that both the CEPD, and the control authorities that form it, have sufficient human, technical and financial resources.

This **document** is located at the [following link](#).

### Regarding the designation and situation of the Data Protection Delegates (DPD)

Within the Coordinated Supervision Framework (CEF), the CEPD annually promotes a common supervision action to be developed voluntarily among the authorities that comprise it. The action promoted for the 2023 financial year was dedicated to knowing the situation of the Data Protection Delegates or DPDs and the AEPD actively participated in said action.

As a result of the previous work, the EDPB adopted its final report of conclusions. This report contains an executive summary, a series of recommendations on this topic, a first annex with statistics and a second annex with reports that 25 DPAS (including the AEPD) have previously carried out in their respective territories.

In this initiative, the Committee has sought to obtain information about the profile, position and work of DPDs; gather the experience and conclusions of the authorities that plan to carry out inspections in this area, are starting them or intend to continue them; raise awareness about the requirements applicable to DPDs; ensure that they fulfill the key role assigned to them and evaluate current needs.

The DPAS have been preparing this report, within the Committee, throughout 2023. Once adopted, the EDPB is open to updating it if necessary.

This **report on the designation and situation of DPOs** can be found at the [following link](#).

## STATEMENTS

### Statement 1/2023 on the first review of the operation of the adequacy decision for Japan

In January 2019, the European Commission approved Japan's adequacy decision. This adaptation provided for a review after two years, a review that was carried out in 2021.

As a result of the review, the European Commission prepared a draft report on which it sought opinions from representatives designated by the EDPB and finally published its final report on April 3, 2023.

The aforementioned report is positive and includes the progress that Japan has made in this regard, such as, for example, through the adoption of new regulations, thus strengthening the legal framework around data protection, aligning it even more with EU standards.

Based on the above, the EDPB has made a statement of support, requesting that the next review be carried out within four years.

This **declaration 1/2023** can be found at the [following link](#).

### ChatGPT Taskforce

The CEPD Plenary decided to create on 04/13/23 a specific structure, called "Task Force".

(TF) to coordinate the local sanctioning files opened by the control authorities of the European Economic Area (EEA) on the processing of personal data carried out by the North American entity Open AI (OAI) in the ChatGPT service.

The EDPB made this decision since, until February 15, 2024, OAI did not have an establishment within the EEA, which prevented the activation of the

called the GDPR single window mechanism, also known as One-Stop-Shop, or OSS, for its acronym in English.

This OSS mechanism provides a formal coordination channel between the control authorities concerned in each file to agree on draft decisions related to cross-border data processing.

Consequently, it was necessary to create a coordination system between the control authorities, outside the OSS, to harmonize the decisions that the respective control authorities must make in the future regarding this service. From

Since its creation, this group has held regular meetings exchanging information.

### § 8.1.2 Taskforce on competition, consumption and data protection

**Five meetings** of this group have been held during 2023.

It was decided by the group to designate national contact points in the consumer and competition authorities to carry out the development of the work. The AEPD already has national contact points in the CNMC and in the Single Liaison Office for Cooperation for Consumer Protection (CPC) of the General Directorate of Consumption (Ministry of Social Rights, Consumption and Agenda 2030). Meetings have been held with the members designated for this cooperation and the AEPD has been joining the meetings of the CNMC and the CPC in international forums.

A first questionnaire has been circulated by the CEPD Secretariat to determine the forms of cooperation between the national administrative authorities of the Member States involved within the CEPD, which has been circulated to the CNMC and CPC for completion.

The AEPD has also participated in the meeting of the European Commission's Consumer Working Group on the new cases presented to the EU COM in relation to the obligations of transparency and legitimacy of the business models of digital service platforms.

It has also participated in the meetings of the High Level Group of the European Commission for the execution of the Digital Markets Law of the EU.

#### § 8.1.3 Taskforce on cooperation of EDPB members in other international forums

The AEPD has participated in a total of **3 meetings** during 2023.

The AEPD, as a member of the board of the Consultative Committee of Convention 108 of the Council of Europe (T-PD), has been informing the group about the work of the Committee.

The representation of the AEPD in the T-PD was commanded by it to report on the work within the CAI (Committee on Artificial Intelligence of the Council of Europe). The AEPD is part of the delegation of the Kingdom of Spain in the CAI and in this capacity has been participating in its meetings aimed at the preparation of the first artificial intelligence convention of the Council of Europe.

The AEPD has been regularly informing the international affairs taskforce of the European Data Protection Committee about the results of the drafting of this draft of the convention. The AEPD has been receiving timely information on the work of UNESCO, OECD, Global Privacy Assembly (GPA), G-7 and G-20 on data protection and privacy.

#### § 8.1.4 High Level Group for improving the implementation of police and judicial cooperation in the EU

The AEPD has participated in **2 meetings of the European Commission's Working Group of Senior Experts** to improve the execution of police and judicial cooperation in the EU. He also participated in the **meetings of the three Work subgroups** from the GTA.

The group's objective is to improve the access of national police and judicial forces, EUROPOL and Eurojust to the necessary operational data managed by OTTs and SPIs (large electronic service providers and platforms) for the purposes of operational analysis and investigation into cybercrime. and fight against terrorism and organized crime and against serious crimes.

#### § 8.1.5 High Level Group for the application of the Digital Markets Law of the European Union

During 2023, the AEPD has participated in **three meetings** of the European Commission's GAN on the application of the Digital Markets Law (DGA).

Among other issues, the creation of two working subgroups has been discussed in order to analyze the correct interpretation of art. 5.2 and 7 of the European Digital Markets Law.



## § 8.2. Supervision of the Cooperation IT Systems Police and Judicial Area of Freedom, Security and Justice – new Committee Coordinated Supervision

### § 8.2.1 Coordinated Supervision Committee (CSC)

During 2023, the Coordinated Supervision Committee continued to assume supervision of the different “large IT systems of the Union.”

European Union” through the current common authorities for the supervision of computer systems in the field of police and judicial cooperation of the European Union:

- **SIS II** (Schengen system),
- **VIS** (visas),
- **Eurodac** (immigration),
- **JSA and JIS** (customs),
- **Europol** (European police)
- **Eurojust** (European judicial cooperation body).

The activities of the European Public Prosecutor's Office and the IMI (Internal Market IT system) are also subject to coordinated supervision.

For this reason, references to the common authorities of the IT systems of Europol, Eurojust and SIS II that have already passed to the new supervision coordinated under the CSC are removed in this 2023 annual report.

During 2023, the Committee has developed the activities included for said year in its work program for the period 2022-2024, which establishes the activities to be carried out within the framework of the supervision of the aforementioned computer systems. A total of four in-person meetings and monthly meetings have been held in remote format.

In these meetings, the new supervision framework for the different systems has been developed.

In the field of general supervision of systems, joint workshops have been designed on strategies for the supervision of large IT systems in the field of police and judicial cooperation and an initiative plan has been developed for the participation of society. civil.

Within the framework of the latter, the participation of civil society actors such as NGOs (e.g.: STATEWATCH) and professional associations, etc., has been invited.

In relation to the IT **SIS II system**, a first workshop was held with case studies on the audit exercise in the SIS II system. Questionnaire models have also been developed to monitor the application of specific articles of the SIS Regulation, such as art. 36 on alerts on specific control and harmonized models for the collection of statistical data from the system.

In relation to the **EUROJUST** system, the formulas for cooperation between judicial authorities have been discussed and in particular the agreements with joint investigation teams with third States and the data protection clauses to be included in said agreements.

On the other hand, the discussion of the design of activities for monitoring the processing of data of minors by data protection authorities has also been the subject of attention by the CSC.

The use of secure data communication channels and the improvement of message exchange in SIENA by **EUROPOL** and judicial authorities in the framework of data exchanges by joint investigation teams was also the subject of study by of the Committee.

As regards the IT **EUROPOL** system, the Committee discussed with the EDPS the findings of the annual report on operational data processing within the **EUROPOL** framework. Among the issues discussed, data transfers to police forces of third States with a level of data protection within the framework of police cooperation procedures stand out.

The issue of the processing of data of minors in these procedures was also addressed, the need for legality of these treatments and their proportionality in accordance with the jurisprudence of the CJEU. There is special concern about the use of minors in organized crime and particularly in specific crimes such as robbery of private homes. The delegations studied the harmonization of the processes for entering alerts into IT systems in the case of minors involved in crimes at very young ages.

In relation to the European Public Prosecutor's Office EPPO, the AEPD has been following the deployment of the national EPPO offices and in particular the Spanish office. The CSC has also monitored the joint inspection carried out by the Portuguese data protection agency and the European Data Protection Supervisor at the EPPO office in Portugal.

The CSC has also continued discussing, in view of the result of the inspection, the execution needs of the single national offices of the EPPO.

## 8.2.2 VIS Supervision Coordination Group (VIS SCG)

During 2023, the Agency has continued its work on the **VIS SCG** within the framework of the 2022-24 program approved in the 2023 financial year.

As a continuation of the Schengen audit of Spain carried out between March 20 and 25, 2022, which included the audit of the VIS visa system, the AEPD has had meetings with the authorities of the Ministry of Foreign Affairs in the field of activities consular offices to continue with the action plan to monitor and follow-up the application of the protection of personal data in the field of visa granting. This activity has followed the recommendations approved by the VIS SCG in the 2022-24 action plan.

The AEPD has also participated in the discussions on the new common inspection plan of the VIS system, which is established as a coordinated activity under the direction of the Portuguese Data Protection Agency.

Within the framework of the SCG VIS meetings, the European Commission has been regularly reporting on its inspections and audits. He has also reported on the development of work on his proposal for a "European digital visa".

## 8.2.3 Coordination Group of the Eurodac Supervision (GCS) (fingerprint information system)

During 2023, the AEPD participated in the **two annual meetings of the GCS Eurodac** in the European Data Protection Committee.

In 2023, the program for the 2022-24 period has been continued, which develops the following issues.

1. The entry into force and application of the Interoperability Regulation, and its effect and interaction with the Eurodac Regulation.
2. The suggestion of topics to be discussed during Eurodac inspections at the national level, in order to provide guidance to the Control Authorities.
3. The activity of the Eurodac SCG within the framework of coordinated supervision within the framework of CEPD.
4. The issue of fake HITs.

In this framework, the AEPD informed the EURODAC Coordination Supervision Group about the AEPD's future inspection of the Eurodac national contact point in compliance with the agency's action plan for the supervision of police cooperation IT systems. and judicial.

The data protection authorities were informed by EU-LISA about the incidents in the system and in particular about the errors or "false positives" that occurred during the year 2023.

The GSC also dealt with the access of police forces and judges to the EURODAC system. Finally, the GSC approved the 2020-21 activity report and its publication in the DOCE.

At the request of the GSC, the influence of the interoperability regulation on the operation of the Eurodac IT system and the EU screening and Eurodac Regulations was also discussed in view of the Schengen report of May 16, 2023.

It was decided to closely monitor the process and study the impact of these regulations at the national level. A working group has been formed for this matter within the GSC.

## 8.2.4 Participation of the AEPD in others international forums

### 8.2.4.1 Council of Europe

#### Consultative Committee and Bureau of Convention 108+ of the Council of Europe

During 2023, the Spanish Data Protection Agency participated in the two ordinary meetings of the Advisory Committee as a Plenary and in the three meetings as a Table.

In 2022, the Board, the governing body of the work of the Advisory Committee, was renewed. The Agency is part of the Board as one of the members of the Spanish delegation has been elected as a member of it.

Since the election of members is carried out in a personal capacity, the Agency continued to have two members on the Committee with representation in the Plenary and Board.

As mentioned in the 2021 report, the Spanish State ratified Convention 108+ on January 28, 2021, which has been deposited.

By the end of 2023, a total of 43 States parties have signed the convention, of which 28 have also proceeded to ratify it. 3 observer states are also signatories to the convention: Argentina, Uruguay and Mauritius.

Below are the **documents approved by the Council of Europe regarding the protection of personal data** during the 2022-23 financial year:

- Second module of the Council of Europe Standard Contractual Clauses for international transfers of personal data.
- Recommendations on data protection in the processing of personal data to combat money laundering, counterfeiting and the financing of terrorism.
- Approval of the resolution of the Convention Bureau to begin work on recommendations regarding the protection of personal data in the context of neurosciences.

#### Artificial Intelligence Committee

The Committee on Artificial Intelligence represents the 46 States party to the Council of Europe that are members of the Committee and seven States that have observer status. Its mission is to prepare a consolidated draft text of the first convention of the Council of Europe on artificial intelligence that will be presented to the Committee of Ministers of the Council of Europe in May 2024. The Convention has a deadline for submitting the draft to the assembly in March 2024.

The European Commission is leading the negotiations in collaboration with the delegations of the EU Member States that are parties to the CAI Committee.

The AEPD has participated in a total of 16 meetings of the Committee to prepare the text of the draft of the convention in the form of a Plenary and Editorial Board.

- 8.2.4.2 Global Privacy Assembly (GPA)

The 45th Annual Meeting of the Global Privacy Assembly took place this year in Bermuda from October 15 to 20.

In this edition the following **resolutions were approved** :

- Resolution on AI and employment.
- Resolution on Health Data and Scientific investigation.
- Resolution on the achievement of global Data Protection standards.
- Resolution on the GPA library.
- Resolution on generative AI systems.
- Resolution on the establishment of a working group on the intersectional gender perspective in data protection.
  
- Resolution Award on Privacy and Human Rights.

In addition to the previous resolutions, the GPA approved its Strategic Plan for the period 2023-2025.

All these **documents** are accessible at the [following link](#).

- 8.2.4.3 International Working Group on Data Protection in Technology – Berlin Group

The International Working Group on Data Protection in Technology (IWGDPT), also called the “Berlin Group”, focuses its attention on trends and developments in the technology sector, such as "Big Data", the "Internet of Things or IoT" or artificial intelligence. To this end, the group develops recommendations and guidelines to use these technologies in accordance with data protection requirements.

In its joint work, the Berlin Group benefits from its heterogeneous and transnational composition, with participants coming from data protection supervisory authorities, government agencies, international organizations and non-governmental organizations, as well as from research and the world. academic. The AEPD especially appreciates the exchange of opinions and cooperation with international colleagues to achieve the most complete and favorable recommendations for the protection of data on new technologies for an international audience such as the target audience of the Berlin Group. It meets twice a year in different parts of the world.

The 2023 meetings took place in Rome (Italy) and Ottawa (Canada).

During the year 2023, the **Berlin Group approved and published** the following **documents**:

- Working document on telemetry and diagnostic data.
  
- Working document on “smart cities”.

These **Berlin Group documents** are accessible at the [following link](#).

## 9. Cooperation with Latin America

### 9.1. RIPD meeting February 2023

On **February 27 and 28, 2023**, the Meeting of the Ibero-American Data Protection Network (RIPD) was held in Santa Cruz de la Sierra (Bolivia).

At the Meeting, the new national legislative developments in the Region were reviewed and the panels were developed: **“From theory to practice. Adopting regional mechanisms to promote international data transfer”** in which the problem of international transfers was addressed. **“Data protection in health”**, where the impact and regulation of artificial intelligence in the health field were discussed. **“Security Gaps”**. **“The protection of people in the digital sphere, initiatives of the control authorities.”** A series of presentations were also developed on proactive responsibility in data protection, privacy by design and by default, impact assessments in the private and public sphere. There was a space dedicated to Civil Society on digital gender violence. In the closed session, the INAI was renewed as Presidency of the RIPD and the strategy to follow to achieve a statement from the IACHR on the right to data protection was defined.

### 9.2. Coordinated action RIPD. Artificial Intelligence - ChatGPT

On **April 27**, at the initiative of the RIPD Presidency and Secretariat, a meeting of RIPD authorities was held in order to address the problems associated with the ChatGPT service. It was agreed to cooperate effectively regarding the actions of the authorities within the framework of their national powers. This action is the first coordinated research action that is developed within the framework of the RIPD and its 2021-2025 Strategic Plan.

### 9.3. RIPD coordinated action. CoIDH Application

Request for Advisory Opinion prepared jointly by the INAI and INCAM whose purpose is to make a formal request to the Inter-American Court of Human Rights (CoIDH) so that it can rule, through an Advisory Opinion, regarding the interpretation of the essential content and scope of the fundamental right to the protection of personal data, in light of the content of article 11 of the American Convention on Human Rights (CADH).

### 9.4. 20th anniversary meeting RIPD

The Meeting has served to strengthen alliances and support the various entities that make up the RIPD. In the field of international organizations, we must highlight the collaborations in the aforementioned Meeting of organizations such as the Organization of American States, the Federal Trade Commission, the Organization for Economic Cooperation and Development, the United Nations Organization through its Special Rapporteur for Privacy, the Council of Europe, the European Commission or the European Data Protection Supervisor. Alliances have been reinforced with other international Data Protection Networks that had direct participation in the Meeting: The Personal Data Protection Commission of Singapore, representing ASEAN Association of Southeast Asian Nations and the National Commission for the Moroccan Personal Data Protection Control, as Permanent Secretariat of the African Data Protection Network.

During the Meeting in question, which has come to be considered as a “refoundation of the RIPD”, consensus has been reached by the Authorities of the Region on the modification of the Statutes of the Network to update them based on criteria common. There has also been an emphasis on the

need for the “internationalization of the RIPD” through collaborations and agreements with other global data protection networks, as well as increasing its visibility in the Region.

A declaration on Neuro-rights has been approved through which the RIPD adheres to the declarations of the Inter-American Juridical Committee of the OAS.

#### • **Creation of four working groups:**

- ChatGPT
- Neurodata
- Digital Violence and Digital Health
- WorldCoin

#### • **RIPD web update.**

• **RIPD web repository management** including tools and guides developed in the countries of the Region.

• In April 2024, a **workshop will be held in Lima, Peru** to analyze the progress of the four working groups and the adherence to the Model Contractual Clauses by the National Authorities of the Region.

• In May 2024, the **2024 Meeting** will be held, in which the final wording of the new RIPD Regulations and the documents with the results of the four working groups would be approved.



For more information about this RIPD 20th anniversary meeting, see the [following link](#).

## • **9.5. InterCoonecta Program 2023 of the AECID**

Presentation to the InterCoonecta Program and award.

Within the framework of this program whose main objective is democratic governance and technical training of the Authorities of the Region, 4 training courses will be developed for the staff of the entities guaranteeing Data Protection and will support the development of the annual RIPD Meeting 2024.

## • **9.6. SEGIB call**

Within the framework of the SEGIB call, of which the AEPD has been awarded as Permanent Secretariat of the RIPD, the actions corresponding to the **two categories have been carried out:**

- **Dissemination.** Through the RIPD XX Anniversary Meeting. These funds have supported the financing of the 20th anniversary Meeting, facilitating the participation of Authorities from the Region.

- **Training.** Study Visit by the AGETIC of Bolivia.

## • **9.7. Webinar**

Webinar on the adequacy agreement on data protection between the European Union and the United States government called EU-US Data Privacy Framework.

## 9.8. Collaborations

In order to analyze synergies and collaboration possibilities in terms of data protection and within the framework of the internationalization process of the RIPD, the **following actions and meetings** have been carried out with International and Regional Organizations:

- **Costa Rican Authority.** Management with the CoE accession Costa Rica agreement 108+
- **Latin American University of Science and Technology.** Costa Rica. Collaboration for internship, dissemination and training.
- **International IDEA.** Participation in seminar rivers.
- **SEGIB.** Ibero-American Charter of Principles and Rights in Digital Environments. Collaboration in matters of Data Protection. Participation in seminars.
- **Singapore Personal Data Protection Commission,** representing ASEAN Association of Southeast Asian Nations.
- **National Commission for the Control of the Protection of Personal Data of Morocco,** as Permanent Secretariat of the African Data Protection Network.
- **California Privacy Agency (CPA).**
- **Federal Trade Commission.**
- **UNESCO.** Collaboration in LAC and EU in Neuro-technologies and Artificial Intelligence.
- **Organization of American States.** Collaboration in Neurorights.
- **European Commission.** Cross-border flows in the Region.

# THE AGENCY IN FIGURES



# 1. Data inspection

## 1. The beginning of the supervisory power.

### Claims, communications and actions on own initiative

The Subdirector General of Data Inspection (SGID, hereinafter) is the body dependent on the Director of the Agency that, in the event of possible violation of the regulations or failure to pay attention to the exercise of rights, analyzes the evidence, carries out the actions of appropriate evaluation or investigation and, when appropriate, instructs the appropriate procedures to propose to the Director the adoption of the corresponding resolution.

Complaints can be received directly at the Agency, which is the most common situation, although they can also come through a Control Authority of one of the Member States of the European Economic Area (EEA). The latter have a cross-border nature and are admitted through the single window mechanism, established in article 60 of the GDPR: they are complaints submitted in another Member State of the EEA or actions that a Control Authority (CA) of the EEA has decided to initiate by own initiative and in which citizens or establishments of the person responsible in Spain are affected. For this reason, the SGID also evaluates its participation in the initiation of cooperation procedures for cross-border cases in which other CAs notify us of an alleged infringement. The cases received from other CAs show an increasing trend in recent years.

Either as a consequence of the complaints, or on its own initiative, the Agency may determine the opening of investigative actions to achieve a better and more concrete determination of the facts that may infringe data protection regulations, as well as the identification of the person responsible. During the year 2023, the number of investigations that have been carried out on their own initiative has increased slightly compared to 2022.

Among the cases in which action is taken on its own initiative, it is worth highlighting the investigative actions that are carried out, when appropriate, following notifications of personal data breaches. Notifications are made in accordance with article 33 of the GDPR. These notifications are received in the first instance in the Technological Innovation Division (DIT) of the AEPD and, after a first analysis, when there are objective data that justify a more in-depth analysis, the Director agrees to initiate an ex officio investigation and urge the SGID to begin the preliminary investigation actions aimed at proving the facts.

Although above these variations, what stands out the most in terms of its volume and level of growth and what has the most impact on the start of new cases in 2023 has been the very high increase in claims received at the Agency.

The following table shows these data and their comparison with those of the previous exercise:

Table 1: Entries of new cases to inspection					
Entry type	2021	2022	2023	% relative	ÿ% annual
Claims* submitted to the AEPD	13,905	15,128	21,590	97%	43%
Cross-border cases from other EEA CAs	581	651	708	3%	9%
Own initiative of the AEPD (inc. gaps)	85	43	fifty	0%	16%
<b>TOTAL</b>	<b>14,571</b>	<b>15,822</b>	<b>22,348</b>	<b>100%</b>	<b>41%</b>

\* Includes complaints in which the personal data does not concern the applicant

The upward trend in recent years is strongly accentuated in the number of entries received, especially in complaints, which represent 43% more than in 2022 and 55% more than two years ago. Thus, for the third consecutive year, a record is broken in terms of the number of complaints received by this Agency, already more than double those received in 2020.

The Agency has been in existence for 30 years and, along this path, the increase in complaints has been a constant, accompanying the successive regulatory reforms, and the social evolution itself and the greater risks of the treatments, due to the volume and extension. of the data generated and the ubiquity of the new services and devices that process it. But the growth that has been observed since the beginning of this decade has never been experienced. The evolution of claims in these 30 years is reviewed in [Annex B: Evolution of claims 1993-2023](#).

## Claims submitted to the AEPD



Although the increase in cross-border cases is more moderate, 9% (22% compared to 2021), these types of claims are significantly more costly both in time and effort of the Agency's staff. This is so as there is a need to reach consensus with other EEA authorities.

In 2023, despite the extraordinary increase in inflows, the SGID has been able to increase its resolution capacity to more than 20,000 complaints, leaving the rate of complaints resolved compared to complaints received at 94%, thus preventing the number from of pending claims will end the year in numbers that are difficult to assume. However, despite all the effort that has been made, unresolved claims at the end of the year are more than 4,900, 32% higher than the previous year's figure.

This year's challenge was huge, and the possibility of collapse in the SGID, a reality. The claims resolved during the year were 37% higher than the previous year, which demonstrates the aforementioned effort on all fronts: organizational, technological, personnel, etc. The following table shows the figures related to the complaint resolution rate:

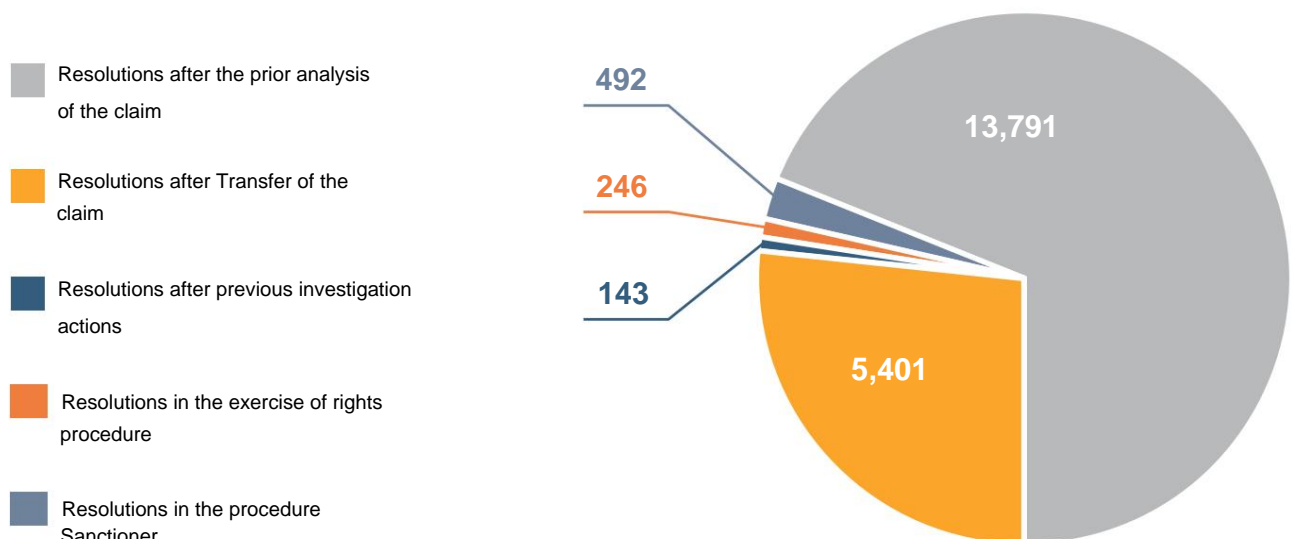
**Table 2: Resolved and pending claims**

Complaint resolution rate	2021	2022	2023	ÿ% annual
Claims* resolved during the year	14,098	14,937	20,391	37%
Claims pending resolution at the end of the year 3,516		3,707	4,906	32%
Rate of resolved claims vs. received in the year	101%	99%	94%	-5%

\* It includes any claim for violation of regulations, regardless of whether the personal data concerns you.

## ÿ 2. Resolutions

### Claims resolution phase



One of the indicators that show the activity carried out by the General Subdirectorato of Data Inspection is the number of resolutions that are issued. The entries reflected in the previous section can give rise to different actions and procedures that end in resolutions. The number of entries processed does not necessarily have to coincide with the number of resolutions signed: several claims referring to the same infraction and subject claimed can be grouped together and, on the contrary, multiple claimants may appear in one claim, giving rise to multiple procedures and, therefore, therefore, at different resolutions.

## 2.1 Resolutions during the prior Analysis of the Claim

The first phase carried out in the processing of claims is the initial analysis of each of them. It includes its classification, the formal verification of its content and the analysis of competence and other causes that affect its foundation and admissibility. This is what is called the phase of prior analysis of the admissibility of the claim.

If the analysis shows that the claim does not meet the admissibility requirements established in the regulations, it will be inadmissible and, if not, it will advance to the next phase, where the evaluation of admissibility will continue. The main reason for inadmissibility is that there are no rational indications of the existence of an infringement within the Agency's jurisdiction. This year 2023, the percentage of resolutions in this phase has increased to 69%. The increase derives from the large number of complaints received during the year, many of which do not meet the requirements to be processed, as they do not provide all the necessary information that allows rational indications of the existence of an infringement to be appreciated. In this sense, the Agency is putting great effort into ensuring that the claims it receives are complete, providing the minimum documentation necessary to be admitted, and that claims are not received that will not be able to bear fruit (because they do not involve an infringement, because they are not within of the Agency's competence, due to lack of evidence, etc.). In this sense, the [resolution approving the claim presentation models](#) was published in 2023, detailing the information that claimants must provide so that their claim can take effect.

The following table shows the data regarding the resolutions:

Table 3: Resolutions in the prior analysis phase of the claim				
Result type	2022	2023	% relative	ÿ% annual
<b>Resolutions after the claim analysis phase*</b>	<b>8,190</b>	<b>12,416</b>	<b>66%</b>	<b>52%</b>
<b>Inadmissibility for processing</b>	7,928	12,135	65%	53%
<b>Competition from other national ACs (CGPJ, Autonomous AC)</b>	262	281	2%	7%
<b>Resolutions in other phases</b>	<b>5,436</b>	<b>6,282</b>	<b>3. 4%</b>	<b>16%</b>
<b>TOTAL</b>	<b>13,626</b>	<b>20,073</b>	<b>100%</b>	<b>37%</b>

\* Includes claims related to the exercise of rights.

The main reason for inadmissibility for processing is that there are no signs of infringement regarding the protection of personal data. In this regard, it is very important that citizens include in their claims the necessary evidence that demonstrates the facts claimed, and along these lines work is being done so that the entry of claims through electronic headquarters is carried out in a guided manner, so that the citizen understands. Firstly, if there is an infraction that you can complain to the Agency and, if there is, it must be accompanied by the necessary documentary support.

## 2.2 Later resolutions

With the entry into force of the RGPD and the LOPDGDD, a phase was introduced for transferring the claim to the person responsible or in charge of the treatment or, where appropriate, to the DPD, with the aim of resolving claims more quickly, in accordance with the provisions of article 65 of the LOPDGDD. These transfers can lead to the solution of the claim, or to provide information that helps clarify the situation so that it can be determined that there has been no violation of data protection regulations. In this way, it is possible to resolve a high number of complaints in a short time, regardless of the inspection action, which can always be carried out in accordance with the powers attributed to the SGID.

The inclusion of the transfer phase has represented a great improvement in relation to previous work procedures. In 2023, after having proceeded to transfer the claim, a resolution was issued ending its processing in 86% of the cases, thus giving a faster response to the claimants than that achieved with the previous regulations and solved in a more rapid way. agile your claim.

The increase in the percentage of claims that are resolved in early phases (admissibility analysis and transfer of the claim) has led to a consequent reduction in the number of prior investigation actions and procedures. This allows the SGID to respond to the greater complexity of the treatments analyzed with an adequate distribution of the available resources, since these subsequent actions require a significant dedication of time and people.

The greater effectiveness of the actions is reflected in the reduction of archiving resolutions of previous investigation actions. Investigations end in a higher percentage in the opening of procedures, therefore fewer prior investigative actions are initiated that do not achieve their main objective: determining the violation and the offender.

For its part, the Agency considered the existence of responsibilities that had to be resolved in a sanctioning procedure in 8% of the resolved cases. It should be noted that in 2023, the LOPDGDD has given regulatory coverage to the new Warning procedure, separate from the sanctioning procedure. Given that only three resolutions have been made with this new procedure due to the short periods that have elapsed since its approval, their number is reported in the report added to those of the sanctioning procedure. On the other hand, the regulatory changes also affect the sanctions imposed on public administrations, which will be resolved from now on with the declaration of infringement, thus reserving the figure of the warning to the cases in which the opening of a procedure of infringement is considered. warning, for any type of responsible subject.

The following table shows the complete distribution of resolutions that are made after the prior analysis of the claim, according to the phase in which the case is finalized.

Table 4: Resolutions in phases subsequent to the prior analysis of the claim				
Result type	2022	2023	% relative	ÿ% annual
<b>Resolutions after Transfer of the claim*</b>	<b>4,268</b>	<b>5,401</b>	<b>86%</b>	<b>27%</b>
Satisfactory response from the person in charge or manager	2,912	3,475	55%	19%
Be fully competent with another CA in the EEA	411	531	8%	29%
Act as interested authority in the EEA (provisional file)	196	274	4%	40%
Other reasons after transfer**	749	1,121	18%	fifty%
<b>Resolutions after previous investigation actions*</b>	<b>288</b>	<b>143</b>	<b>2%</b>	<b>-fifty%</b>
Archive of previous research actions	288	143	2%	-fifty%
<b>Resolutions in the procedure Exercise of rights</b>	<b>305</b>	<b>246</b>	<b>4%</b>	<b>-19%</b>
Resolved in the procedure for exercising rights	305	246	4%	-19%
<b>Resolutions after sanctioning procedure</b>	<b>575</b>	<b>492</b>	<b>8%</b>	<b>-14%</b>
Resolved in sanctioning procedure - Fine	385	367	6%	-5%
Resolved in sanctioning procedure - Warning or declaration of violation	126	61	1%	-52%
Resolved in sanctioning procedure - Archive	64	64	1%	0%
<b>TOTAL</b>	<b>5,436</b>	<b>6,282</b>	<b>100%</b>	<b>16%</b>

\* Includes claims related to the exercise of rights.

\*\* It includes complaints from the State Security Forces and Bodies and from citizens whose right to data protection is not affected by the infringement, which ends with the person responsible being informed of his obligations in relation to the reported infringement, the regulations to which that must be complied with, and the warning that if it is not adjusted, the pertinent actions may be initiated.

## 2.3 Average resolution times

The average times, in days, until the final resolution is issued are reflected below. It must be taken into account that resolutions made before admission for processing are inadmissible. This occurs during the evaluation of the claim, that is, after the previous analysis or after the transfer of the claim to the controller or processor.

In the prior analysis phase of the claim, the average time corresponds to the time from when the claim is received until its inadmissibility is resolved, after analyzing the formal verification of the content and its basis. It should be taken into account that article 65.5 of the LOPDGDD establishes a period of 3 months for this concept.

**Table 5: Average resolution time in previous analysis**

Average resolution times in the Analysis phase (in days)	2022	2023	ÿ% annual
Resolutions after Analysis of the claim*	25	32	28%
<b>HALF TIME</b>	<b>25</b>	<b>32</b>	<b>28%</b>

\* Includes claims related to the exercise of rights

The increase in prior analysis times derives directly from the flow of claims received in 2023, which has exceeded the capacity of the dedicated resources, and even the implementation of a shock plan in which extra effort was requested from staff to stop the accumulation of complaints at the entrance.

Taking into account the increase in the workload in 2023 (claims an increase of 43% in the entry of claims, which has meant a 52% increase in resolutions in the prior analysis phase) and the increase in staff in the subdirectorate, which, compared to this, has been only 20%, the resulting average number of days has increased less than what would correspond proportionally to the increase in workload per person. This caveat is equally applicable to the rest of the resolution times broken down below.

In the phase of transferring the claim to the person in charge or in charge, the average time corresponds to the time from when the claim is received until the resolution of inadmissibility is signed, after transfer to the person in charge and the analysis of the response received. The average time is less than the three months provided by the regulations for admission to processing, although it is again longer than the previous year for identical reasons.

Once these two phases have been passed, the claim is accepted for processing and the procedures established in the Law begin. The resolution times in previous investigation actions, in procedures for the exercise of rights and in sanctioning procedures, are counted from the date of admission to processing the claim until the resolution is signed.

The global average resolution time has increased, although very slightly compared to 2022. This data changes the downward trend in resolution times that has been achieved in recent years, a direct result of the exponential increase in claims, as well as as well as the increase in complexity of the data processing carried out and which in turn determine a greater complexity of the investigations and procedures of this Agency.

**Table 6: Average resolution time according to the procedure in which it is resolved**

Average resolution times according to the procedure (in days)	2022	2023	ÿ% annual
Resolutions after Transfer actions*	82	91	eleven%
Resolutions after previous investigation actions	262	269	3%
Resolutions in the exercise of rights procedure	84	110	31%
Resolutions in the Sanctioning procedure	242	292	twenty-one%
<b>HALF TIME</b>	<b>109</b>	<b>112</b>	<b>3%</b>

\* Includes claims related to the exercise of rights

### ÿ 3. Actions carried out

The figures shown below give a perspective of the total actions carried out in the General Subdirectorate of Data Inspection, regardless of whether or not they finalize the file and, therefore, whether or not they give rise to resolutions. An example of this would be a transfer of a claim that does not bear fruit, or prior investigation actions that give rise to a sanctioning procedure. These actions do not generate a resolution and, therefore, are not detailed in the previous section, but they do involve a procedure that is reported in this section. In the case of procedures for the exercise of rights, sanctions or appeals for reconsideration, which always put an end to the administrative procedure and therefore produce a resolution, the figures coincide with those given in the previous section.

It should be noted that the number of claims evaluated in the prior admissibility analysis phase may vary compared to the number of claims presented in the year, since it is a procedure that has an average duration of 31 days as indicated below. Therefore, the year begins by analyzing pending claims from the last month of the previous year, and in the same way the year ends without being able to conclude the analysis of the total claims submitted in the last weeks of the year.

A strong increase in actions can be observed in the early stages, consistent with the large increase in claims submitted, as well as the increase in resolutions in the phase of transferring the claim to the controller or processor. Continuing with last year's trend, the number of investigative actions has decreased. The reasons are several, mainly due to the increase in resolutions in previous phases, and the criteria followed for its initiation: its rigor has increased, accompanied by greater depth in the investigations. The latter has had a direct effect on the percentage of investigations that culminate in sanctioning procedures, increasing by 10 points compared to the previous year, and 21 compared to 2 years ago. The reduction in sanctioning and rights procedures also derives from the increase in resolutions in previous phases, to which is added in the case of the exercise of rights a decrease in claims specifically related to them.



The increase in the number of appeals processed is also consistent with the increase in the number of resolutions issued.

**Table 7: Actions carried out**

Number of actions completed according to the phase of the procedure	2022	2023	ÿ% annual
Prior analysis of admissibility of claims*	14,654	21,156	44%
Transfer actions*	5,150	6,281	22%
Previous research actions	476	316	-3. 4%
Procedures for exercising rights	305	246	-19%
Sanctioning procedures	575	492	-14%
Replacement resources	735	940	28%
<b>TOTAL</b>	<b>21,895</b>	<b>29,431</b>	<b>3. 4%</b>

\* Includes claims related to the exercise of rights

### ÿ 3.1 Average processing times

The times that appear in this section measure the average times of actions of each of the individual phases related to the management of the claim. These average times are measured in days from the beginning of each phase to its completion. The same cause that was explained when describing the increase in average resolution times naturally applies to each of the phases of the procedure.

**Table 8: Average processing times**

Average times of actions carried out in the management of the claim according to the phase of the procedure (in days)	2022	2023	ÿ% annual
Claims analyzed*	24	31	32%
Transfer actions*	57	56	0%
Previous research actions	200	206	3%
Procedures for exercising rights	67	84	25%
Sanctioning procedures	111	130	17%
Replacement resources	86	106	23%
<b>HALF TIME</b>	<b>40</b>	<b>43</b>	<b>7%</b>

\* Includes claims related to the exercise of rights

## 4. Public administrations sanctioned for non-compliance with requirements and measures

In relation to the effectiveness of the Agency's actions and resolutions, the SGID supervises compliance with the information requirements made under the investigative powers regulated in article 58.1 of the RGPD, and the adaptation measures to the regulations imposed in the resolutions in accordance with the corrective powers regulated in article 58.2.

The lack of response to information requests represents an infraction classified in article 83.5.e) of the RGPD, classified as very serious for the purposes of prescription in article 72.1 of the LOPDGDD.

For its part, the lack of accreditation of the corrective measures imposed represents an infraction classified in article 83.6 of the RGPD, also classified as very serious for the purposes of prescription in article 72.1 of the LOPDGDD.

The following table reports on the public officials who have been sanctioned by the Agency for the infractions described during the year 2023. In accordance with article 77 of the LOPDGDD, they are sanctioned by declaring the infraction.

**Table 9: Public Administrations sanctioned for non-compliance with requirements and corrective measures**

investigated	Entity type investigated	Article infringed	Typification article	Resolution
City Hall of Las Palmas de Gran Canaria	Administration Local	GDPR 58.2	83.6	<a href="https://www.aepd.es/document/ps-00619-2022.pdf">https://www.aepd.es/document/ps-00619-2022.pdf</a>
Andalusian Public Foundation for the Management of Health Research Seville (Fisevi)	Administration Autonomous	GDPR 58.1	83.5	<a href="https://www.aepd.es/document/ps-00220-2023.pdf">https://www.aepd.es/document/ps-00220-2023.pdf</a>
Los Llanos de Aridane City Council	Administration Local	GDPR 58.2	83.6	<a href="https://www.aepd.es/document/ps-00234-2023.pdf">https://www.aepd.es/document/ps-00234-2023.pdf</a>
Department of Education, Culture and Government Sports Aragon	Administration Autonomous	GDPR 58.2	83.6	<a href="https://www.aepd.es/document/ps-00238-2023.pdf">https://www.aepd.es/document/ps-00238-2023.pdf</a>
Ministry of Health of the Community Board of Castilla la Mancha	Administration Autonomous	GDPR 58.2	83.6	<a href="https://www.aepd.es/document/ps-00241-2023.pdf">https://www.aepd.es/document/ps-00241-2023.pdf</a>

## 5. Resources

The appeals filed against resolutions of the SGID procedures are shown below, depending on whether they were for reconsideration, extraordinary review, or contentious-administrative.

**Table 10: Resources presented to the Agency**

Resource type	2022	2023	ÿ% annual
Replacement resources	898	952	6%
Extraordinary review resources	12	16	33%
Contentious-administrative resources	115	128	eleven%
<b>TOTAL</b>	<b>1025</b>	<b>1,096</b>	<b>7%</b>

The increase in resources is not surprising if it is correlated with the increase in the number of resolutions issued by the Agency.

The replacement and review appeals resolved annually by the AEPD are shown in the following table.

A significant increase can be seen in the increase in resolved appeals, greater than the increase in appeals presented to the Agency. This is because a significant effort has been made, with some organizational changes, aimed at trying to resolve this increase in resources.

**Table 11: Resolved resources**

Resource type	2022	2023	ÿ% annual
Replacement resources	735	940	28%
Extraordinary review resources	eleven	18	64%
<b>TOTAL</b>	<b>746</b>	<b>958</b>	<b>28%</b>

## 6. Classifications

### 6.1 Most frequently raised complaints

The 10 areas of activity with the highest number of complaints received in 2023 are shown, which together account for just over 80% of the total complaints received in the year:

Table 12: Most frequent complaints				
Most frequently raised complaints	2022	2023	% relative	ÿ% annual
<b>TOP 10</b>	<b>12,020</b>	<b>17,431</b>	<b>81%</b>	Four. Five%
Advertising (except spam)	2,000	4,279	twenty%	114%
Internet services	2,221	2,897	13%	30%
Video surveillance	2,197	2,843	13%	29%
Commerce, transport and hospitality	906	1,504	7%	66%
Financial entities/creditors	767	1,362	6%	78%
Delinquency Files	1,159	1,263	6%	9%
Debt Claim	910	975	5%	7%
Health	543	803	4%	48%
Public administration	796	802	4%	1%
Laboral things	521	703	3%	35%
Others	3,108	4,159	19%	3. 4%
<b>TOTAL</b>	<b>15,128</b>	<b>21,590</b>	<b>100%</b>	<b>43%</b>

The increase in complaints received in relation to receiving unwanted advertising stands out. And this is despite the efforts that have already been made by the AEPD to promote mediation mechanisms in this type of conflict. The vast majority of these complaints relate to telephone calls and are mainly related to the telecommunications sector or water, gas or electricity supplies. The approval of the new regulation on advertising calls in Law 11/2022, of June 28, General Telecommunications (LGTel), which came into force during 2023, has generated an increase in this type of claims, given that They have continued to receive these types of calls, even though a different effect was expected.

In general, and given the large increase in the number of complaints, it is not surprising that all the rest of the activity groups have also seen an increase. Although this is especially true in the commerce, transport and hospitality sector (+66%), where the increases in claims against courier or parcel companies are notable; and the financial entities sector (+78%), mainly related to the exercise of rights.

## 6.2 Most frequent areas in sanctioning procedures

The 10 areas of activity with the highest number of sanctioning procedures completed in 2023 are shown, representing 86% of the total sanctioning procedures resolved in the year:

Table 13: Most frequent sanctioning procedures

activity group	2022	2023	% relative	ÿ% annual
<b>TOP 10</b>	<b>465</b>	<b>419</b>	<b>86%</b>	<b>-10%</b>
Video surveillance	164	164	33%	0%
Internet services	88	70	14%	-twenty%
Public administration	53	31	6%	-42%
Advertising (email/SMS spam)	29	28	6%	-3%
Fraudulent hiring	17	27	6%	59%
Telecommunications	eleven	27	6%	145%
Commerce, transport and hospitality	twenty-one	26	5%	24%
Laboral things	27	18	4%	-33%
Advertising (except spam)	23	14	3%	-39%
Security Bankruptcies	32	14	3%	-56%
<b>Others</b>	<b>110</b>	<b>71</b>	<b>14%</b>	<b>-35%</b>
<b>TOTAL</b>	<b>575</b>	<b>490</b>	<b>100%</b>	<b>-fifteen%</b>

Video surveillance procedures continue to stand out, many of which are related to neighborhood communities or private homes, followed by those related to Internet services, although the number of these sanctioning procedures has decreased compared to the previous year. Although the largest number of complaints filed is related to unwanted advertising and

that the vast majority are related to calls from the telecommunications sector or the water, gas or electricity supply sector, the number of sanctioners related to this case does not have such a high relative percentage; This is because in many cases those responsible for the calls are not in Spain or cannot be identified.

## 7. Cross-border area (EEA)

The application of the GDPR develops in Chapter VII the cooperation mechanisms between control authorities of the European Economic Area, in which the Regulation is fully applicable.

### 7.1 Cross-border cases with the participation of the AEPD

In cases with cross-border components that affect citizens or establishments of responsible parties in Spain, the AEPD participates in their resolution. Depending on whether the controller's main establishment is in Spain or in another Member State, in accordance with the single window mechanism, participation will be as the main or interested authority respectively.

**Table 14: Cross-border cases participated**

Role of the AEPD	2022	2023	Yearly % annual
New cases led as primary authority	fifteen	25	67%
New cases in cooperation as interested authority	201	301	fifty%
<b>TOTAL</b>	<b>216</b>	<b>326</b>	<b>51%</b>

Of the cases in which Spain has acted as the main authority, the following procedures should be highlighted, for the amount of the fine imposed:

**Table 15: Main cross-border cases in which the Agency has been the main authority**

Responsible	Infringement	Penalty fee
OPEN BANK, SA	Art. 25 and 32 of the RGPD	€2,500,000
GLOVOAPP23, SL	Art. 13, 25, 32, 35 and 5.1.e) of the RGPD	€550,000
THE MAIL TRACK COMPANY	Art. 13, 14, 5.1.a) and 6.1 of the RGPD	€100,000

You can read more about these and more cross-border cases participated as a leading authority in section "6.2 Most relevant claims and procedures".

Regarding the cases in which Spain has participated as an interested authority, given its relevance and amount of the fine imposed, the following cases are worth highlighting:

**Table 16: Main cross-border cases in which the Agency has been an interested authority**

Responsible	Penalty fee
FACEBOOK IRELAND LIMITED	€1,200,000,000
TIKTOK	€345,000,000
INSTAGRAM	€180,000,000
WHATSAPP INC	€5,500,000

The processing of these procedures was carried out by the Irish authority, in cooperation with the AEPD and other authorities of the European Economic Area. The resolutions have been published by the authority of that country and are collected in the [repository](#) of the European Data Protection Committee.

## 7.2 Requests received related to the Cooperation procedure

In addition to the single window mechanism developed in Article 60, the GDPR also regulates other cooperation mechanisms in Chapter VII. The procedures of articles 61 and 62 can be requested even for local cases.

The following information compiles both new cases from other control authorities, as well as other requests for assistance and consultation received by the AEPD, as well as the draft decisions analyzed and participated in by the AEPD. Inflows from other EEA states stabilize with a slight increase of 1%. The entry of new cross-border cases and consultations from other authorities increase, but the draft decisions of cases in which the AEPD participates are reduced. Since this last assumption is a complex process that can last several years, the decrease in decisions in the year depends on the initiation of cases in previous years.

**Table 17: Requests and decisions received in cooperation procedures**

Entry type	2022	2023	ÿ% annual
Cross-border cases from other CAs	651	708	9%
Assistance requests from other CAs	311	294	-5%
Consultations of other CAs in cross-border procedures	48	51	6%
Decision projects of cases in which the AEPD participates*	132	99	-25%
Joint operations in which the AEPD participates	0	0	0%
<b>TOTAL</b>	<b>1,142</b>	<b>1,152</b>	<b>1%</b>

\* The draft decisions received, even if issued by the main one, involve subsequent negotiation and consensus work among all participating authorities and require a large amount of resources and effort.

### 7.3 Requests sent related to the Cooperation procedure

Finally, the same table as in the previous section is shown, with the opposite view: the cases, requests, queries and draft decisions issued by the AEPD to the rest of the European control authorities.

The greater volume of cases and consultations with other authorities (+40%) derives fundamentally from the increase in claims and files processed by the SGID in 2023. Regarding the decisions led by the AEPD, a greater number of cases have been resolved this year. cross-border procedures, some of which had been initiated in previous years. The draft decisions issued by the AEPD involve additional work of negotiation and consensus between all the participating European authorities, which extends the deadlines necessary for their resolution.

**Table 18: Requests and decisions submitted in cooperation procedures**

Notification type	2022	2023	ÿ% annual
Cross-border cases shared with other CAs	24	64	167%
Requests for assistance to other CAs	93	102	10%
Consultations with other CAs in cross-border procedures	18	10	-44%
Case decision projects led by the AEPD	25	48	92%
<b>TOTAL</b>	<b>160</b>	<b>224</b>	<b>40%</b>

### 7.4 International working groups

In addition to the negotiation and consensus work in each cross-border file in which the Agency has participated, the SGID has also been present in different sessions of working groups dependent on the European Data Protection Committee (CEPD).

**Table 19: European working groups with the participation of the SGID**

Workgroup	Purpose
Cooperation Expert Subgroup	Focus the procedures established by the GDPR for the purposes of the cooperation mechanism. Provide guidance on procedural issues related to the cooperation mechanism. Provide international mutual assistance and other cooperation tools to enforce the GDPR outside the EU (Article 50 GDPR).
Enforcement Expert Subgroup	Analyze the need for additional clarifications or guidance, based on practical experiences with the application of chapters VI, VII and VIII of the GDPR. Evaluate possible updates to the existing tools of the cooperation subgroup. Track research activities. Ask practical questions about research. Provide guidance on the practical application of Chapter VII of the GDPR, including exchanges on specific cases. Provide guidance on the application of Chapter VIII of the GDPR together with the Working Group on Administrative Fines. Analyze the procedures of article 65 and article 66.



**Table 19: European working groups with the participation of the SGID**

Workgroup	Purpose
<b>IT User Expert Subgroup</b>	Develop and test computer tools used by the CEPD with a practical approach. Collect feedback on the IT system from users. Adapt systems and manuals. Discuss other business needs, including teleconferencing and video conferencing systems.
<b>Taskforce on Administrative Purposes</b>	Develop guidelines for the harmonization of the calculation of fines.
<b>Cookie Banner Task Force</b>	Exchange points of view on legal analysis and possible infringements. Provide support to activities at the national level. Streamline communication.
<b>101 Complaints Task Force</b>	
<b>Support Pool of experts</b>	Help supervisory authorities increase their capacity to supervise and enforce the safeguarding of personal data.
<b>Information system Schengen –SIS-</b>	Establish coordination meetings of the second generation Schengen Information System –SIS II- with the national SIS II authorities within the framework of the planning of the Schengen evaluation.
<b>GDPR Fine Tuning</b>	Propose an adaptation of the RGPD in those aspects related to cross-border issues.

## 8. Fines

### 8.1 Evolution of fines imposed

The following figures refer to the economic sanctions imposed in a final resolution, regardless of their state of execution and collection:

**Table 20: Volume of fines**

Evolution of fines imposed	2022	2023	∆% annual
<b>Number of fines</b>	378	367	-3%
<b>Total</b>	20,775,361	€29,817,410	44%

The total amount increases significantly compared to the previous year, despite the aforementioned reduction in the number of sanctioning procedures, all due to the greater complexity of the treatments analyzed, their greater scope, and therefore greater impact of the infractions. Fines exceeding one million euros imposed on legal entities for resolutions signed in 2023 and that have become final and enforceable are published by the Agency in the BOE, in accordance with the provisions of the LOPDGDD.

Are detailed below:

**Table 21: Fines exceeding one million euros in final and executive resolution**

Responsible	Infringement	Penalty fee
<b>BANCO BILBAO VIZCAYA ARGENTARIA, SA</b>	Art. 6.1 GDPR, art. 25 GDPR, art 32 GDPR	€1,184,000
<b>CAIXABANK, SA</b>	Art. 5.1.f) RGPD, art. 25 GDPR, art. 32 GDPR	€5,000,000
<b>OPEN BANK, SA.</b>	Art. 25 GDPR, art. 32 GDPR	€2,500,000

It should be noted that although the number of complaints has an upward trend and a very strong increase in recent years, and that therefore the number of resolutions issued by the Agency is in line with this data, the amount of the fines does not have to be ascending, given that the fines imposed depend on the infractions committed, the aggravating circumstances that may exist and the persons, natural or legal, who have committed them, given that the fines have to be effective, proportionate and dissuasive, in such a way that a sanction for an infraction is not more profitable than adaptation to compliance with the regulations.

## 8.2 Areas with the highest overall amount of fines

The following table breaks down the 6 areas of activity with the highest amount in sanctions in 2023:

**Table 22: Breakdown of fines by topic**

Amount of fines in euros depending on the issue	2022	2023	% relative	Δ% annual
<b>Six themes with the highest total amount in 2023</b>	<b>€14,241,901</b>	<b>€26,433,600</b>	<b>89%</b>	<b>86%</b>
<b>Security Bankruptcies</b>	€821,800	€12,907,000	43%	1471%
<b>Financial entities / creditors</b>	€596,200	€5,321,000	18%	792%
<b>Data protection rights</b>	€5,900	€2,633,400	9%	44534%
<b>Fraudulent hiring</b>	€706,800	€2,571,500	9%	264%
<b>Telecommunications</b>	€632,000	€1,942,000	7%	207%
<b>Internet services</b>	€11,479,201	€1,058,700	4%	-91%
<b>Others</b>	<b>€6,533,460</b>	<b>€3,383,810</b>	<b>eleven%</b>	<b>-48%</b>
<b>TOTAL</b>	<b>€20,775,361</b>	<b>€29,817,410</b>	<b>100%</b>	<b>44%</b>

The large increase in sanctions in some of these issues compared to the previous year corresponds to individual fines in high-impact procedures.

## Annex A: Priority Channel Data

In 2019, the AEPD created a specific system to pursue the illegitimate dissemination of especially sensitive content that put the rights and freedoms of those affected at high risk, known as the Priority Channel. Additionally, in order to facilitate the communication of this type of case to minors, the requirements for their electronic communications were made more flexible, providing a means of contact based on an open form, without the need to present the claim using a digital certificate.

### A.1 Entries received through the Priority Channel

Below are the inputs received by the two channels referred to above.

Table 23: Inputs received by the Priority Channel			
Entry type	2022	2023	ÿ% annual
Claims submitted to the AEPD	255	413	62%
Communications from the minors channel (14-18 years old)	167	159	-5%
<b>TOTAL</b>	<b>422</b>	<b>572</b>	<b>36%</b>

You can see the total increase in complaints received for these two types of entry. The decrease in communications received through the minor channel is striking, despite the fact that it is one of the infractions that has been increasing lately.

### A.2 Entries processed urgently after the Agency's analysis

Each entry that arrives through the Priority Channel is analyzed in depth to determine if the case meets the characteristics to be treated as sensitive, in which case it is processed urgently. In the rest of the cases, their processing can also continue, although by ordinary means and without the nature of urgency, because, after their analysis, it is observed that they have no relationship with the objective of the Canal. The following table shows the entries that, after said analysis, were channeled through the urgent channel.

Table 24: Entries treated urgently			
Entry type	2022	2023	ÿ% annual
Claims received through the Priority Channel	33	29	-12%
Claims received through ordinary channels	10	7	-30%
Communications from the minors channel (14-18 years old)	17	5	-71%
<b>TOTAL</b>	<b>60</b>	<b>41</b>	<b>-32%</b>

You can see the big difference that exists in relation to the previous table. Many complaints are submitted through this channel, perhaps to be dealt with urgently. However, the prior analysis carried out in the Agency allows us to discriminate and treat urgently only those cases in which sensitive content is being disseminated without consent that could seriously affect the rights and freedoms of those affected.

### § A.3 Interventions carried out on an emergency basis

When the especially sensitive nature of the personal data disclosed is determined and the serious impact on the rights and freedoms of individuals is determined and may cause irreparable harm, it may be necessary and proportionate to carry out an emergency intervention to adopt provisional measures to safeguard the fundamental right to the protection of the personal data of those affected.

In such cases, those responsible are required to remove the sensitive content as immediately as possible. If the person responsible cannot be identified, this request is made to the corresponding service providers. The following table shows the number of interventions carried out on an emergency basis and the cases in which they have proven to be effective, removing the exposed contents.

Table 25: Content removal interventions			
Type of Action	2022	2023	ÿ% annual
<b>Emergency interventions for the removal of content</b>	<b>51</b>	<b>36</b>	<b>-29%</b>
<b>Precautionary measures taken</b>	31	26	-16%
<b>Urgent withdrawal requests sent</b>	twenty	10	-fifty%
<b>Interventions that have been effective</b>	<b>46</b>	<b>3.4</b>	<b>-26%</b>
<b>Precautionary measures that have proven effective</b>	28	24	-14%
<b>Urgent Takedown Requests That Have Been Effective</b>	18	10	-44%

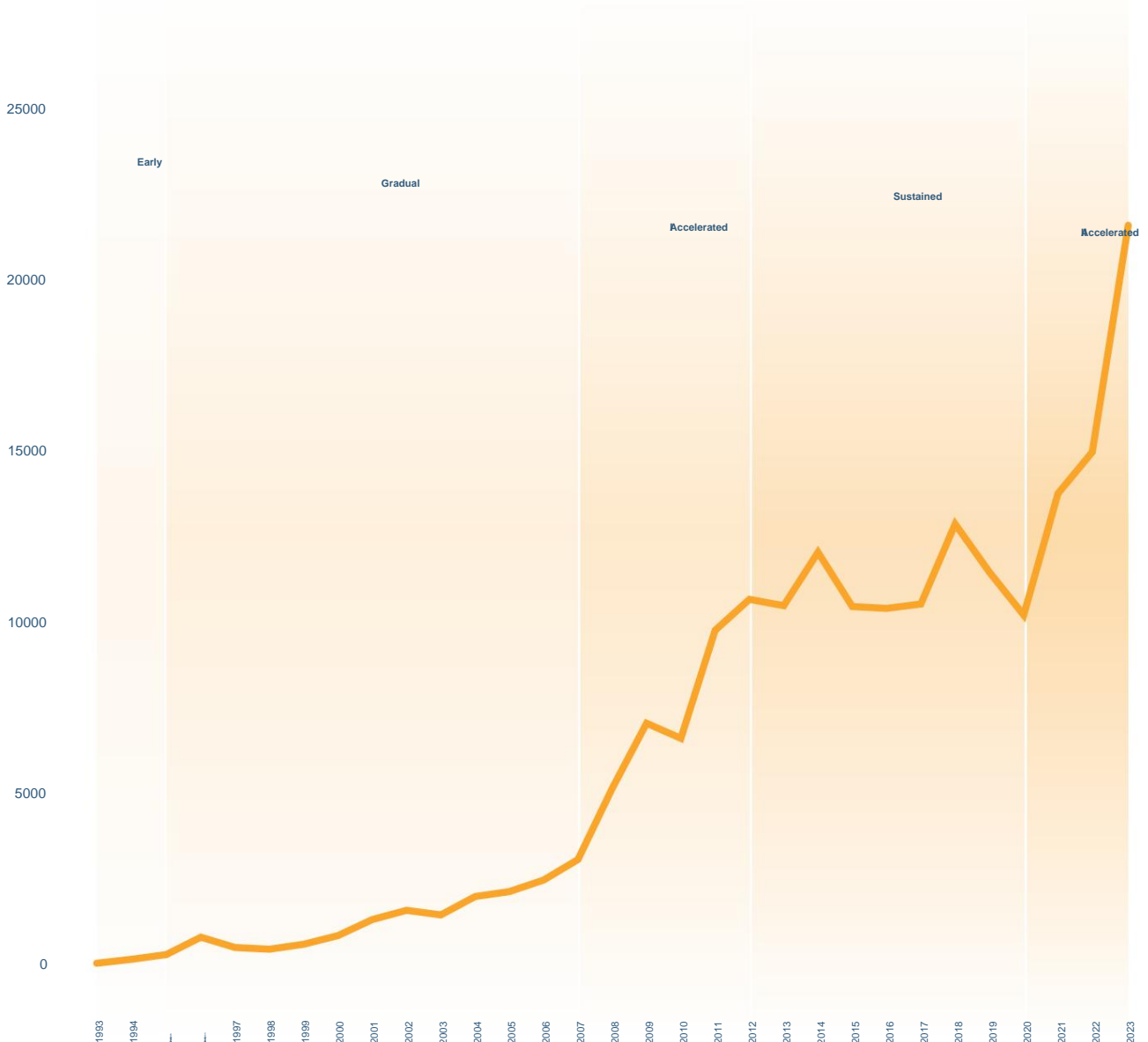
It should be noted that the two precautionary measures that have not been effective during the year were signed during the last days of 2023, which is why at the end of the year they are pending compliance. However, these measures were carried out during the first days of 2024, the precautionary measures have been 100% effective.

## Annex B: Evolution of claims 1993-2023

In this year, when the Agency celebrates 30 years of history, a brief overview of the SGID's activity is presented below through the analysis of the claims it processes. The evolution of the claims presented is a clear reflection of the evolution of the protection of the fundamental right to the protection of personal data, both in the growing awareness of citizens, public powers and social and economic agents regarding its social significance. and individual, as well as the scope and diversity of treatments that affect it.

The growth in claims has been constant over these 30 years, but there have been two periods of sharpest growth that have taken the number of claims to new levels, the second still open at the closing date of this Report.

**Graph 3: Claims presented to the AEPD**



### 📅 Early years (1993-1995)

Even though the first writings containing claims or complaints regarding data protection date back to the end of 1993, it can be said that the Subdirector General of Data Inspection begins to have significant activity in terms of supervision of rights and instruction of sanctioning procedures. In 1994. This year represents significant progress from the point of view of the application of Organic Law 5/1992, on the Regulation of the Automated Processing of Personal Data (LORTAD). During it, the presence of the Data Protection Agency as such has become a reality, it has been provided with the necessary budgetary, building and personnel infrastructure, and the Inspection services have been designed. Likewise, in 1994 the period for initial registration of files in the General Data Protection Registry ends.

Thus, in 1994, 81 complaints were received, rising to 334 in 1995, the first full year in which the Inspection's activity was consolidated.

In these first years, half of the complaints received describe infractions related to data of an economic-financial nature (and, among them, especially those related to solvency, credit and late payment). A significant volume of complaints is also received in relation to unwanted advertising, both that carried out by companies for the promotion and sale of products to their own clients and that carried out in the provision of services of this nature to other companies.

### 📅 Gradual increase (1996-2007)

The volume of claims would gradually increase in the following years, at an average rate of around 25% annually, while the Agency's activity is consolidated and the regulatory framework is deepened.

The year 2000 is a year marked in terms of data protection, by two events of special importance. The entry into force of Organic Law 15/1999, on the Protection of Personal Data (LOPD), in the month of January which, replacing the LORTAD, becomes the main regulatory text on the matter in our country, and the Ruling of the Constitutional Court 292/2000, dated November 30, by which the supreme body for the interpretation of our Constitution comes to define the right to data protection as an independent right in our constitutional system.

The claims received exceeded a thousand for the first time in 2001, continuing this gradual growth until 3,000 in 2007.

Solvency and delinquency files and direct marketing continue to occupy the concerns of citizens during the final years of the 20th century. However, already during the year 2000 there were very numerous inspection actions carried out in relation to activities carried out within the Internet, initiated as a result of complaints filed by citizens, increasingly concerned about the impact that the Internet may have in the protection of their own privacy. In this sense, the subject of the complaints dealt mainly with the improper publication of personal data, the sending of messages through email or the use of data collected over the Internet for purposes other than that for which it was collected. In the first decade of the 21st century, new online services were born and the complaints received due to the impact of these new technologies on the privacy of citizens increased: the dissemination of data on the Internet through eMule, the dissemination of images on YouTube, the Internet email and search engine data retention policies are some of the main areas of complaint in this area.

Complaints are also beginning to be received in significant numbers about treatments carried out by telecommunications operators, a sector that maintains a relevant part of citizens' concerns in the following years, being in 2002 the sector with the highest number of complaints, above the related to solvency and delinquency files. The most significant problem that has arisen in recent years in the telecommunications sector is related to the pre-assignment of telephone lines for the provision of the service by another operator, carried out without the knowledge or consent of the affected party.

The resolutions issued in response to complaints regarding the processing of health data also deserve special attention. Of all the categories of data classified by the LOPD as specially protected data, health data is the one that raises the greatest problems in terms of its protection. The most common complaints are those related to required security measures and the duty of secrecy regarding information related to people's health.

Starting in 2004, complaints related to an area that will grow significantly in the following years began to stand out: video surveillance. In 2007, after experiencing a growth of 412% compared to the previous year, they became one of the most frequent types of claims, driven by the exponential increase in the installation of video surveillance cameras for security reasons.

This activity was usually carried out by the State Security Forces and Corps within the scope of their specific regulation, as well as by financial entities, and in these years it has been extended to other private sectors. The data relating to the owners of video surveillance files are especially significant: after the tourism and hospitality, commerce and health sectors, the communities of owners appear.

### **Accelerated growth I (2008-2012)**

The importance of the functions entrusted to the Agency, its greater presence in society, the attribution of new powers and the increase experienced in its activity mean that, from 2008 to 2012, the rate of entry of claims accelerates with increases in some years 50%, and exceeding 10,000 complaints received for the first time in 2012.

In 2008, the Center for Sociological Research (CIS) included in its February barometer a questionnaire aimed at evaluating citizen awareness of the protection of personal data, resulting in more than 70% of citizens in Spain being concerned about the protection of personal data. data protection and the use of personal information. Likewise, the CIS barometer reflected that 52.4% of Spanish citizens claimed to know the existence of a law that protects them against possible abuses that may occur with their personal data, and placed the percentage of citizens who He claimed to be aware of the existence of the AEPD as the body in charge of defending his rights.

In these years there has also been a growth in claims to protect the exercise of citizens' rights included in the LOPD (Access, Rectification, Cancellation and Opposition), especially those of Access (2 out of 10) and Cancellation ( 7 out of 10). In 2008, procedures for the protection of rights initiated by citizens' claims increased by 88%, and in 2011, up to 35% of the claims received requested protection of the exercise of some of the rights.

This percentage would decrease in the following years.

The most frequent complaints in this period continue to refer to the telecommunications sectors, financial services and solvency files, and video surveillance. The latter is consolidated as a clearly increasing phenomenon.

On the other hand, the growth of the Internet area continues, which represents the fourth area in volume of complaints behind the three mentioned. The evolution of web 2.0 multiplies the offer of new services that are having a massive reception among Internet users (search engines, social networks,...). These services interrelate with each other in such a way that the possibilities of obtaining and processing personal information increase dramatically. The “right to be forgotten” on the Internet became one of the most intense topics of debate in the environment of new Internet services, until its identification by the jurisprudence of the CJEU in 2014.

### • Sustained volume (2013-2020)

From 2013 to 2020, the volume of claims remains around that figure of 10,000 claims, with a clear exception in 2018, the year in which the GDPR begins to apply, which represents a clear promotion of the right to protection of data. data, and the birth of new rights and obligations, receiving more than 13,000 claims that year, 22% more than the previous year.

The application of the GDPR also brought with it new areas of action: cross-border complaints through the single window mechanism and the consequent need for cooperation between European authorities, and investigations of security breaches affecting personal data, which must be notified to the agency.

The Agency's Priority Channel also begins in 2019, to provide an urgent response in the event of illegitimate dissemination of sensitive content, when it seriously affects rights and freedoms or may cause damage that is very difficult to repair.



Thanks to the Agency's intervention, the removal of photographs and videos with sexual or violent content that are viewed on the Internet without the consent of those affected, often belonging to vulnerable groups, is achieved within very short periods of time.

Telecommunications, financial services, video surveillance and internet services continue to be the areas in which the greatest number of complaints occur.

The year 2020 will be strongly influenced by the Covid19 epidemic and the suspension of administrative deadlines, returning to around 10,000 claims. This year, a significant number of complaints were received related to the reconciliation of the guarantee of healthcare and the control of the pandemic with the fundamental right to the protection of personal data.



### 🔍 Accelerated growth II (2021-2023)

The last three years have been marked by a new phase of explosive growth in claims, ending 2023 with a volume that will be close to 22,000 claims, therefore, more than double that of just three years before.

In these years, the most frequent complaints become those related to Internet services, followed by video surveillance and those related to advertising. Between these three areas, 40% of the claims received at the Agency accumulate.

In response to the high number of complaints for receiving unwanted advertising, the AEPD has approved the modification of the code of conduct on data processing in advertising activity promoted by Autocontrol, which includes a way to resolve complaints in this matter more quickly. of data protection and advertising that citizens may raise, and to which, among others, the main telecommunications operators in the country have adhered.

In the Internet field, the risks that the processing of their data on social networks and web pages poses to minors are becoming increasingly important, especially those aimed at adults due to the lack of effective access control. . According to the latest data published by the National Institute of Statistics (INE), for the first time in Spain the proportion of children aged 10 to 15 who have a mobile phone has exceeded 7 out of 10, and 95% have entered on the internet in the last three months. Therefore, it is not surprising that the number of claims in which a minor's right to data protection on the Internet is affected has been increasing, multiplying by two from 2021 to 2023.

Complaints for the processing of biometric data are not yet very numerous in absolute data, but they are also clearly growing, having tripled in these two years, mainly due to their use in identity verification systems for access to all types of facilities, especially in the workplace and related to time control.

Also noteworthy is the significant increase in complaints received regarding commerce, transport and hospitality and, within this area, the increase in reported infractions related to the use of personal data by delivery and parcel companies;

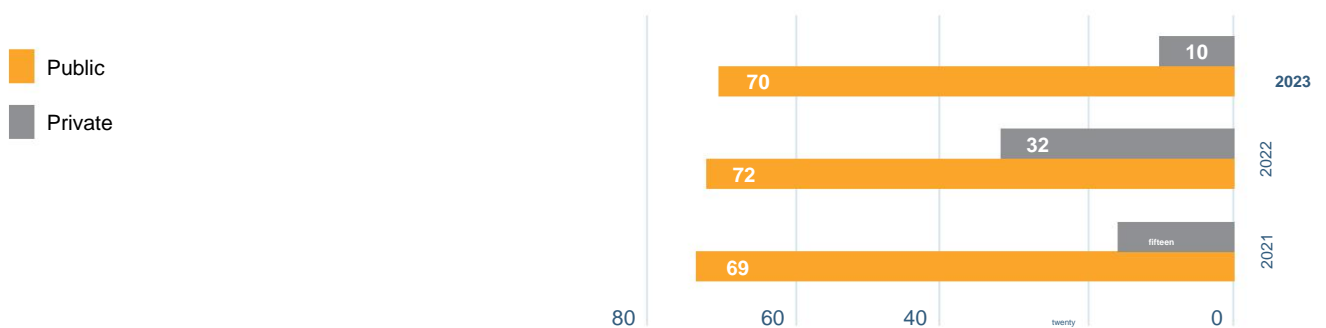
Finally, it is worth highlighting a significant increase in complaints about fraudulent contracting, which mainly concern the energy and telecommunications sectors.

## 2. Legal Office

### Consultations

Public administrations	
AGE	47
CCAA	3
Local entities	1
Public enterprises	3
Other Organizations	16
<b>TOTAL 1</b>	<b>70</b>
Private Consultations	
Associations and Foundations	1
Companies	9
Individuals	0
Unions	0
Others	0
<b>TOTAL 2</b>	<b>10</b>
<b>TOTAL</b>	<b>80</b>

### Query evolution



Evolution of consultations by sectors (2022-2023)		
	2022	2023
Public administrations	72	61
Health / Public Health	1	5
Individuals	1	0
Telecommunications	24	8
Advice and consultancy	0	0
Unions	0	0
Computer Services	0	0
Business associations	0	0
Associations and foundations	3	1
Asset solvency	0	1
Services	0	0
Water and energy	0	0
Security	0	0
Transport	0	0
Financial services	1	1
Investigation	1	0
Courier services	0	2
Insurance	1	2
Political parties	1	0
Owner communities	0	0
Industry and construction	0	0
Education	2	2

*Note: There are queries that deal with more than one sector and are classified in the one that is most relevant. Likewise, other categories are out of use and tend to disappear; they remain the same in comparative terms with the previous year. New ones have been added that in the previous year had 0.*

Evolution of queries by subject (2021-2022)		
	2022	2023
General concepts*	49	49
Area of application	4	1
Legality	eleven	fifteen
Right to Information and Transparency	26	9
Purpose	3	0
Minimization and Proportionality	16	5
Data Accuracy/Quality	6	0
Conservation Period	1	1
Integrity and Confidentiality	0	0
Consent	10	4
Legitimate Interest	1	0
Responsible	4	2
In charge	1	1
Co-responsible	0	1
Rights	3	3
Video Camera Treatments	0	1
Special categories of data	14	13
Safety in Treatment	3	0
Active Responsibility	0	0
Data Protection Delegate	3	3
Risk Management and Impact Assessment	2	0
International transfers	0	0
Transparency and access to public records	0	6

\* **General Concepts:** consultations on draft general provisions are included here.

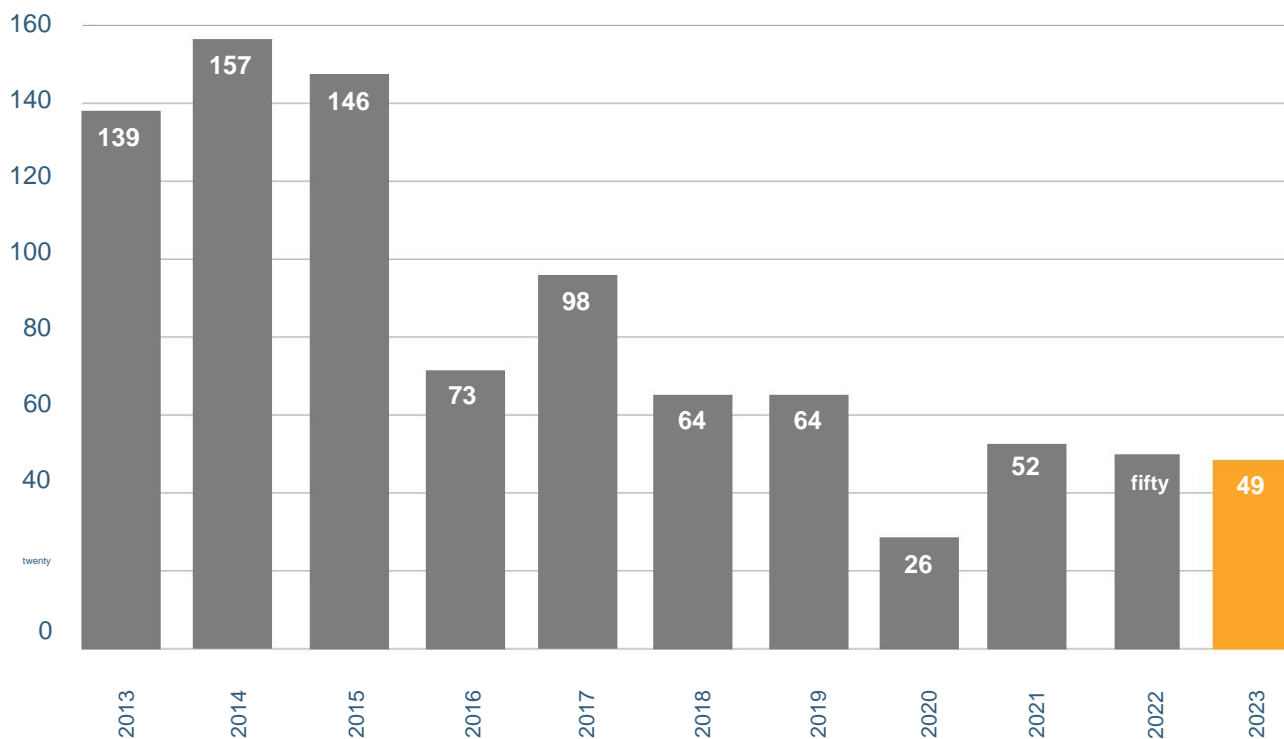
## Evolution of queries by subject (2022-2023)

	2022	2023
Telecommunications	24	12
Minors	0	4
Electronic administration	0	0
Statistics	0	0
Codes of Conduct	3	1

Note: There are queries that deal with more than one subject and that, due to their relevance, appear in more than one section.

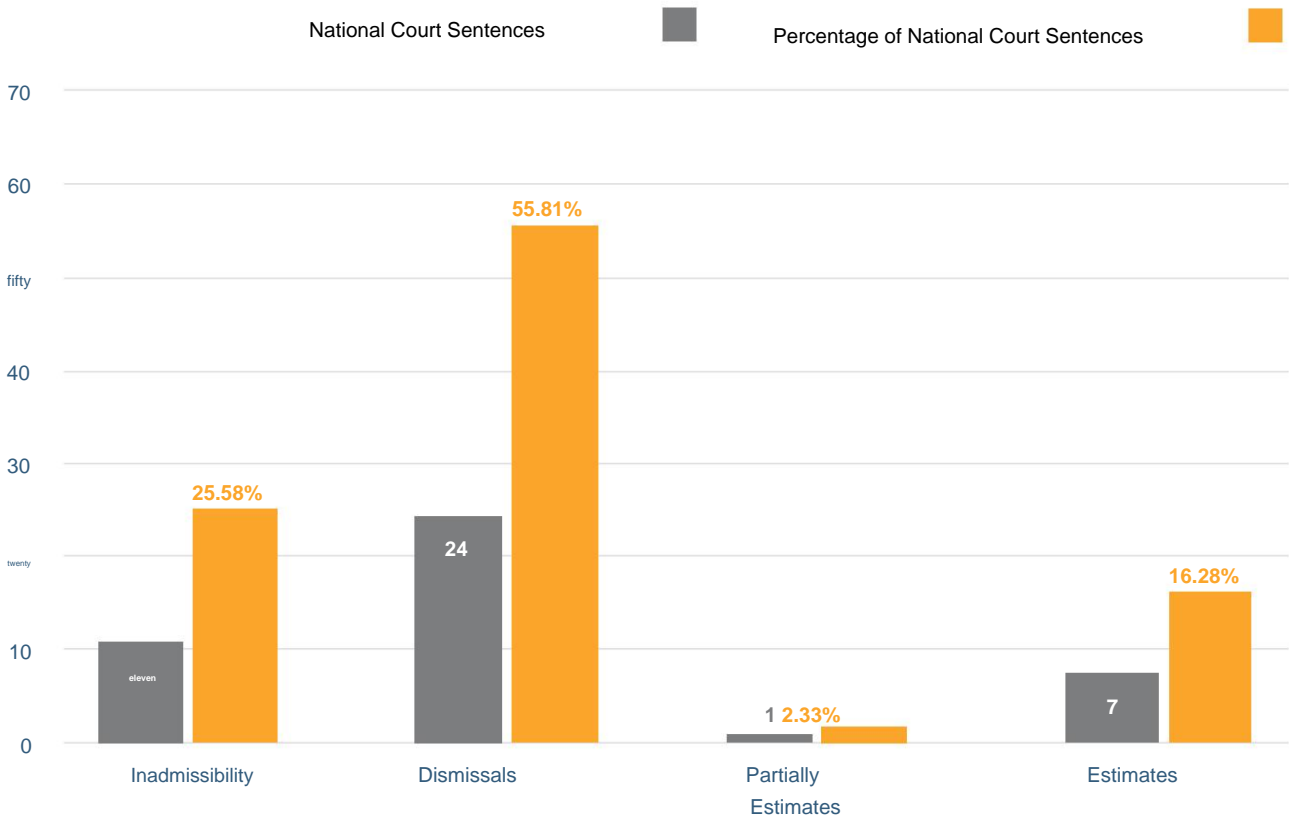
## Evolution from mandatory reports to general provisions (2013-2023)

## General disposition



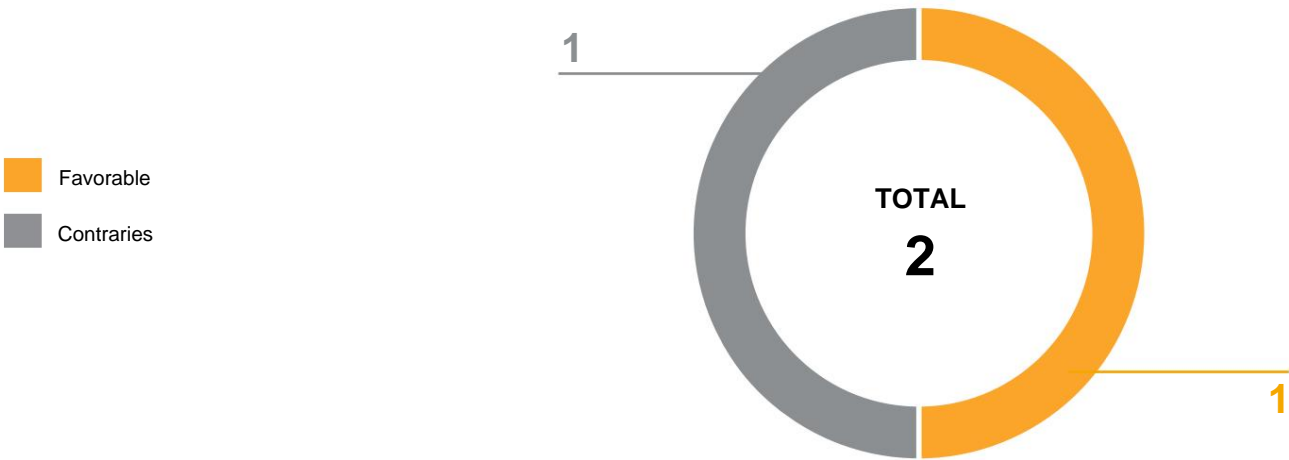
Evolution of mandatory reports (2013-2023)			
Year	General disposition	RD 424/2005	Total
2013	139	seventeen	162
2014	157	23	182
2015	146	fifteen	173
2016	73	23	97
2017	98	28	126
2018	64	24	88
2019	64	12	76
2020	26	fifteen	41
2021	52	5	57
2022	fifty	24	74
2023	49	8	57

### National Court Sentences 2023



**TOTAL National Court Sentences** 43

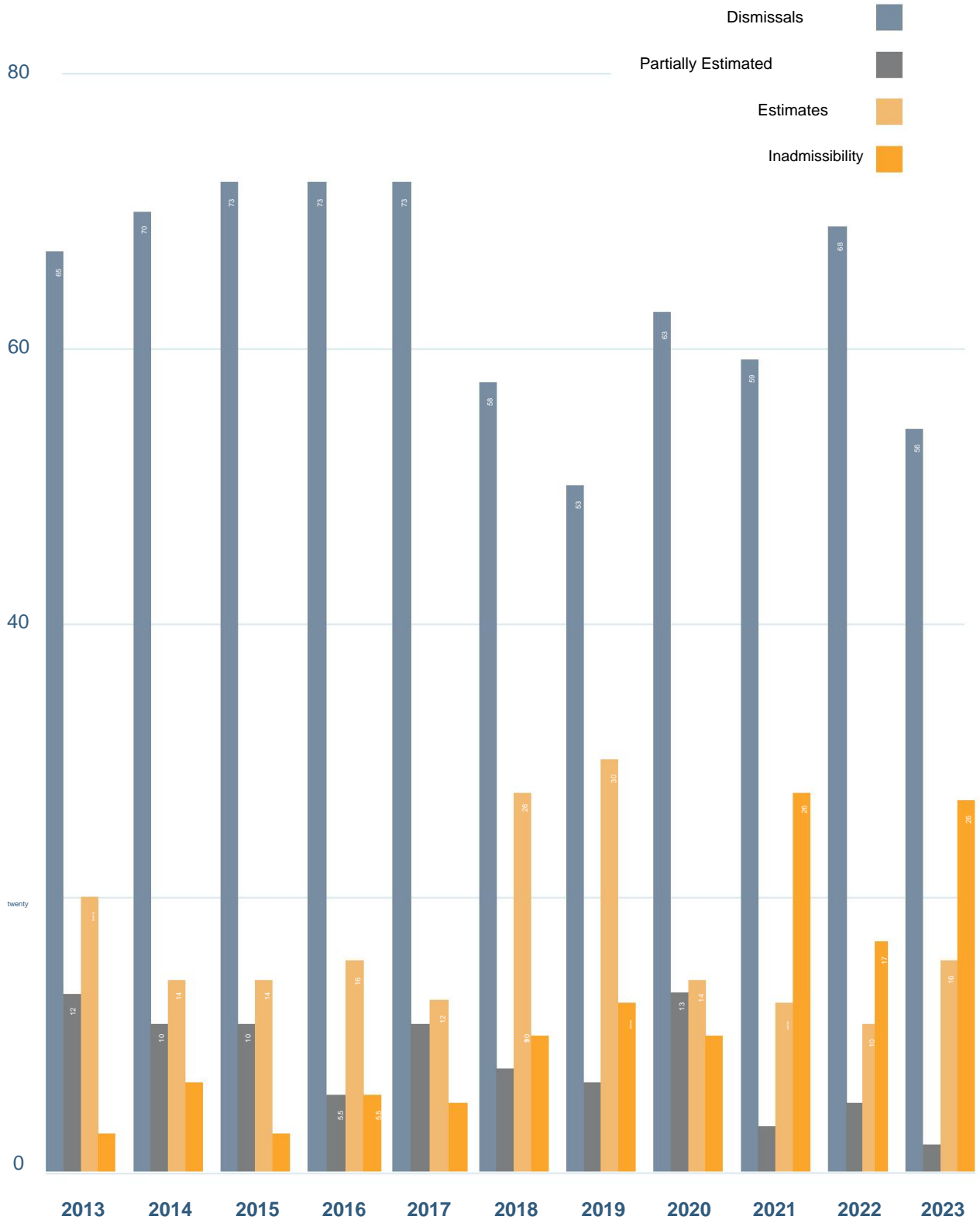
### Supreme Court rulings (2023)



Evolution by direction of failure in percentages (2013-2023)				
Financial year (year)	Dismissals	Partially Estimates	Estimates	Inadmissibility
2013	65	12	twenty	3
2014	70	10	14	6
2015	73	10	14	3
2016	73	5.5	16	5.5
2017	73	10	12	5
2018	58	7	26	9
2019	53	6	30	eleven
2020	63	13	14	9
2021	59	4	eleven	26
2022	68	5	10	17
2023	56	2	16	26



### Evolution by direction of failure in percentages (2013-2023)



Comparison by recurring sector (2022-2023)		
	2022	2023
<b>Individuals</b>	fifty	<b>42</b>
<b>Banking and insurance</b>	1	<b>2</b>
<b>Telecommunications</b>	5	<b>2</b>
<b>Asset solvency and credit</b>	1	<b>0</b>
<b>Distribution and sale</b>	2	<b>0</b>
<b>Water and energy</b>	4	<b>3</b>
<b>Public administrations</b>	2	<b>0</b>
<b>Others</b>	2	<b>6</b>
<b>Associations and unions</b>	0	<b>2</b>
<b>Society of Information</b>	0	<b>2</b>
<b>Advertising and commercial prospecting</b>	2	<b>0</b>
<b>Health</b>	0	<b>4</b>
<b>TOTAL</b>	<b>69</b>	<b>63</b>

*Note: All types of resolutions of the National Court and the Supreme Court, sentences, orders, rulings, organizational measures, etc. are included.*

### 3. Attention to citizens and obligated

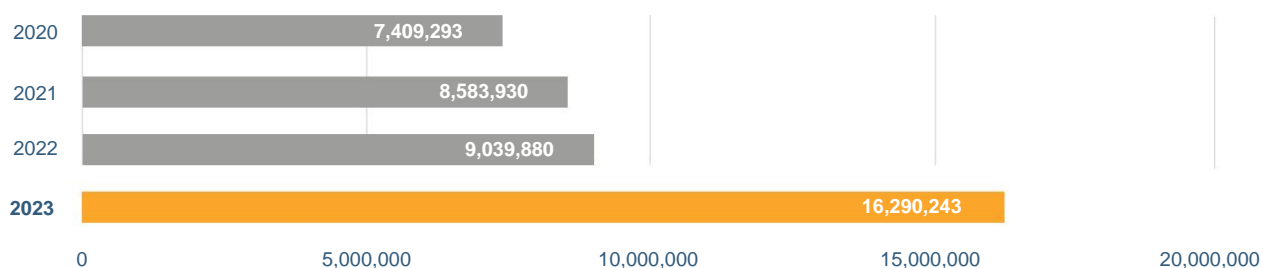
#### subjects

Total queries raised before the Citizen Service area				
	2021	2022	2023	% 2022-2023
In-person	64	110	189	71.82%
Telephones	41,022	42,562	46,958	10.33%
Electronic office and email	3,779	3,766	4,397	16.76%
Chatbot <sup>2</sup> service inquiries			17,337	
<b>TOTAL</b>	<b>44,865</b>	<b>46,438</b>	<b>68,881</b>	<b>48.33%</b>

<sup>1</sup> Includes queries from the citizen service channel (3,411); as well as the complaints and suggestions addressed in accordance with Royal Decree 51/2005, of July 29, which establishes the general framework for improving quality in the General Administration of the State (136); and also queries from the DPD channel (850).

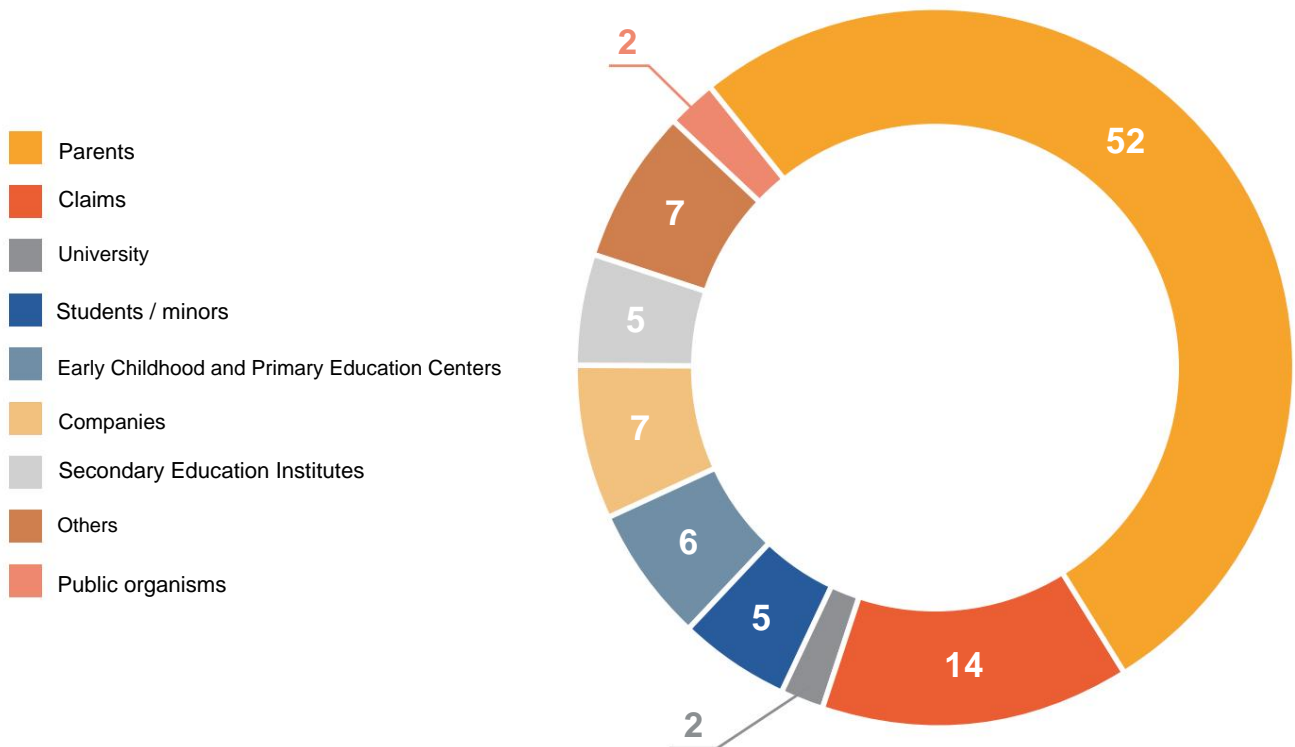
<sup>2</sup> It is a permanent service (24x7) with immediate response with the possibility of referring to an agent. Available on the web from April 12, 2023.

Comparison of visits to the website (www.aepd.es)					
	2020	2021	2022	2023	% 2022-2023
Number of visits	7,409,293	8,583,930	9,039,880	16,290,243	80.20%



Specific queries on the processing of minors' data				
	2021	2022	2023	% 2022-2023
Phone	564	1,243	2,029	63%
WhatsApp	624	607	1,374	126%
Email	366	362	427	18%
Electronic headquarters	235	156	219	40%
<b>TOTAL</b>	<b>1,789</b>	<b>2,368</b>	<b>4,049</b>	<b>71%</b>

Queries by category<sup>3</sup> (in percentages)



<sup>3</sup> This graph is prepared with the queries received in the Education and Minors Area, through the Canal Joven email and electronic headquarters.

Access to the website [www.tudecideseninternet.es](http://www.tudecideseninternet.es)

2023

Number of visits

83,364

## DPD Channel

	2021	2022	2023	% 2022-2023
Consultations	669	695	8504	22.30%

<sup>4</sup> Through the electronic headquarters (718) and derived from other channels (132).

## FAQ Access Report

Number of visits


General Data Protection Regulation. (GDPR)	178,152
Issues about the electronic office	124,322
Minors and education	7,186
Data Protection Officer	66,318
Data processing in the Workplace	62,015
Claims before AEPD and other competent bodies	60,387
Communities of Owners	57,242
Your Rights (Information, Access, Rectification and Cancellation)	56,639
Asset solvency (delinquent files)	50,792
Video surveillance	47,161
International transfers, BCR and Codes of conduct	34,430
Transparency and data protection	29,204
Social networks, illegitimate dissemination of sensitive content	22,564
Health	21,371
Electoral processes	20,287
Unwanted advertising	12,142

TOTAL

910.212

Thematic areas	
Areas of action	Number of visits
Internet and social networks	164,694
A cell phone is more than a cell phone	106,643
Priority channel	90,819
Unwanted advertising	84,952
Health	84,832
Education and Minors	83,364
Video surveillance	68,676
Telecommunications claims	65,563
Public administrations	65,452
Innovation and technology	32,084
Gender violence	30,800

Most consulted topics in telephone service			
Order	Consultation topics	2022	2023
1	Claims	10,023	11,570
2	General Data Protection Regulation (GDPR)	7,272	8,211
3	Rights	5,294	5,503
4	Video surveillance	3,431	3,965
5	Asset solvency files	1939	1,898
6	Owner communities	1,043	1,239
7	EASY TOOL	1,254	1,180
8	Data Protection Officers	1,137	1,089
9	Technical issues of the electronic office	1,220	1,023
10	Data processing in the workplace	468	630
eleven	Transparency and Data Protection	91	77
12	Another questions	3,476	3,875

Web consultation channel with immediate response 24 hours   CHATBOT 			
Order	Query categories	2023	%
1	Claims before the AEPD	3,289	18.97
2	Your rights	2,750	15.86
3	Unwanted advertising	2,122	12.24
4	General data protection regulation	1948	11.24
5	Video surveillance	1,653	9.53
6	Internet and social networks	1,421	8.2
7	Debtor files	1,199	6.92
8	Data protection in the workplace	1,112	6.41
9	Owner communities	747	4.31
10	Education and minors	549	3.17
eleven	Health	547	3.16

Other contents	
Guides	downloads
The guide that does not come with your mobile	425,422
Guide on the use of cookies	350,064
Guide on the use of video cameras for security and other purposes	84,516
Risk management and impact assessment in personal data processing	62,670
Safe purchase on the INTERNET - Practical Guide	59,222
Guide for the person responsible for processing personal data	55,463
Internet Privacy and Security Guide	53,531
Guide for the management and notification of security breaches	52,249
Guide for patients and healthcare users	48,772
Guide for compliance with the duty to inform	46,005
Guidelines for the preparation of contracts between controllers and data processors	42,367
Data protection in labor relations	42,306
Guide on presence control treatments using biometric systems	41,864
Default Data Protection Guide	40,277
Guide for the citizen	38,788
Data protection and Local Administration	35,436
Data protection and crime prevention guide	27,529
Information for sandbox projects for the digital transformation of the financial system	26,005
Adaptation to the RGPD of treatments that incorporate Artificial Intelligence	22,796
Privacy Guide by Design	21,124
Guidance and Guarantees in anonymization procedures	20,765



Other contents	
Guides	downloads
List of elements for regulatory compliance	19,108
Property Managers Guide	16,176
Guide for professionals in the healthcare sector	15,222
Code of good practices in data protection for Big Data projects	15,158
Report on the use by teachers and students of applications that store data in the cloud	14,630
Drones and Data Protection	13,791
Guide for clients who contract Cloud Computing services	13,238
Requirements for Treatment Audits that include AI	11,422
Approach to data spaces from the perspective of the GDPR	9,547
Data protection and crime prevention guide: practical sheets	9,492
Privacy by Design Guide (English version)	9,152
Guide to Technologies and Data Protection in the AA.PP	9,106
10 misunderstandings related to anonymization	8,640
Guide for managing and reporting security breaches (English version)	8,636
Data protection as a guarantee in harassment prevention policies: recommendations from the AEPD	8,251
Guidelines for the validation of cryptographic systems in data protection	8,184
Guidelines for carrying out an impact assessment for data protection in regulatory development	6,911
Guidelines on cookies and web analytics on public administration portals	6,893
Guidance for treatments that involve data communication between Public Administrations faced with the risk of personal data breaches	6,510
How to manage an information leak in a law firm	6,105

Other contents	
Guides	downloads
Risk Management and Impact Assessment in the Processing of Personal Data	5,280
10 Misunderstandings about Machine Learning	5,256
GDPR compliance of processings that embed Artificial Intelligence An introduction	5,218
Guide on the use of cookies (English version)	4,718
Audit Requirements for Personal Data Processing Activities involving AI	4,606
Decalogue of Principles. Age verification and protection systems for minors against inappropriate content	3,592
Guidance for Cloud Computing service providers	3,578
Guidelines for Data Protection by Default	2,976
Drones and Data Protection (English version)	2,185
Accreditation criteria for code of conduct oversight bodies	1920
Technologies and Data Protection in Public Administrations	1,598
10 Misunderstandings about Machine Learning	1,486
10 Misunderstandings Related to Anonymisation	1,431
Guidelines for conducting a data protection impact assessment in regulatory development	<b>1.346</b>
Roadmap to ensure compliance with data protection regulation	905
Age Verification Systems Proof of Concept FAQ (published online 12/14/23)	741
Guidelines on Cookies and Web Analytics in Public Administration Websites	708
Decalogue of principles. Age verification and protection of minors from inappropriate content (published online on 12/18/23)	88
Frequently Asked Questions about the Proofs of Concept of systems for age verification (published online 12/18/23)	83
Technical note with the description of the Proofs of Concept of Systems for Age Verification (published on the web on 12/18/23)	67

Other contents	
Infographics	downloads
Responsibility of minors (and their parents) for acts committed on the Internet	297,657
Information on consent to process personal data of minors	55,914
Decalogue for health and administrative personnel	23,659
Criteria for the processing of personal data in educational centers	23,522
When and how a data breach should be communicated to those affected	22,881
What are your data protection rights	19,833
Family digital plan	16,801
Reference map for treatments that include Artificial Intelligence	15,170
Who is who in the processing of personal data in your educational center	11,215
Performance of the student welfare and protection coordinator	11,150
How do screens affect health?	9,268
Recommendations for users in the use of chatbots with Artificial Intelligence	9,128
The rights you have to protect your personal data	8,109
What should you keep in mind before giving your son or daughter a mobile phone?	7,741
Infographic Protection of minors on the Internet	7,101
Priority channel to communicate the dissemination of sensitive content and request its removal	4,924
Risks associated with age verification systems and summary of the Decalogue of Principles	<b>4,803</b>
Infographic: Measures to minimize online tracking	3,468
10 basic tips to buy safely online	3,292
Risks of the Internet of Things in the home (published on 12/14/2023)	2,279
Data protection on vacation	2,076

## Other contents

Infographics	downloads
How to avoid unwanted advertising	1,623
Infographic: The control is yours, don't let them control you	1,601
Reference Map Personal data processing embedding Artificial Intelligence	1,357
Recommendations for remote contracting of telecommunications and energy services	1,229
Connected toys	1,189
Safe online shopping	996
Facilitate Start	855
Data Protection Regulation	809
Report the dissemination of violent or sexual content on the Internet	646
Infographic: Measures to minimize internet tracking	618
Protect your data when you go back to school	585
Recommendations for users in the use of chatbots with artificial intelligence	568
Strategic Plan Balance	476
Priority Channel - Equality	364
Personal Data Breach Communication	3. 4. 5
Privacy Risks of Internet of Things at Home	301
Risks associated with age verification systems and summary of the Decalogue of principles (published on 12/18/2023)	86

Other contents	
Technical notes	downloads
Protection of minors on the Internet	20,345
Recommendations to protect personal data in mobility and teleworking situations	15,154
K-anonymity as a measure of privacy	9,592
14 mistakes regarding biometric identification and authentication	8,952
The duty to inform and other proactive responsibility measures in apps for mobile devices	8,160
The use of technologies in the fight against COVID19	7,246
Introduction to 5G technologies and their privacy risks	5,931
Measures to minimize online tracking	3,805
K-anonymity as a privacy measure	3,171
Technical note on proofs of concept on age verification systems (Published on 12/14/23)	2,590
DNS Privacy	2,644
Recommendations for the deployment of mobile applications in access to public spaces	2,466
User control in ad personalization on Android	2,432
The duty to inform and other accountability measures for mobile devices	1,437
Preview of the IMDEA NETWORKS and UC3M study: "Analysis of Pre-installed Software on Android Devices and its Risks for User Privacy"	1,332
App access to screen on Android devices	1,134
Preview of "An Analysis of Pre-installed Android Software and Risks for Users' Privacy", an study by IMDEA NETWORKS and UC3M	945
Introduction to 5G technologies and their risks in terms of privacy	937
User controls for ad personalization on Android	893
14 misunderstandings with regard to biometric identification and authentication	861

Other contents	
<b>Technical notes</b>	<b>downloads</b>
DNS Privacy	801
Guidelines for social distancing and access control apps due to COVID-19	743
Measures to minimize internet tracking	710
Technologies in the fight against COVID19	645
Access to applications on the screen for Android devices	512
Recommendations to protect personal data in situations of mobility and telecommuting	483
<b>Other publications</b>	<b>downloads</b>
Report on internet privacy policies. Adaptation to the GDPR	12,925
Introduction to hashing as a personal data pseudonymization technique	10,482
Guidelines for the application of the eighth additional provision and the twelfth final provision of the LOPDGDD	9,305
Compliance with regulations at 'zero cost' and other fraudulent practices	8,730
Fingerprinting or device fingerprint	7,879
Administrative, disciplinary, civil and criminal consequences of the dissemination of sensitive content	7,167
FAQ about COVID-19	6,646
Privacy Shield Override FAQs	5,898
Decalogue for the adaptation to the RGPD of internet privacy policies	5,745
LOPD: News for the Public Sector	5,554
Ex-officio inspection plan for social and health care	4,152
Fingerprinting or Fingerprint of the device (English Version)	3,399
LOPD: News for the Private Sector	3,007
LOPD: News for citizens	2,700

## Other contents

Other publications	downloads
25 years of the Spanish Data Protection Agency	2,386
Ex officio inspection plan on remote contracting in telecommunications operators and energy marketers	2,287
Ex-officio sectoral inspection plan for Public Hospitals	2,199
Analysis of information flows in Android	1954
Introduction to the Hash function as a personal data pseudonymization technique	1901
Analysis of information flows on Android (English Version)	1,611
FAQ about COVID-19	1,363
Survey on the degree of preparation of Spanish companies before the RGPD (AEPD-CEPYME)	1,180
Guidelines for Implementation of the Eighth Additional Provision and Twelfth Final Provision of the LOPDGDD	644
Memories	downloads
AEPD Report 2022	60,865
Social Responsibility Report 2022	32,445

## Digital pact for the protection of people

Digital pact for the protection of people	2023
Member entities (total)	509



Codes of Conduct 5					
	Approved Modified		Inadmissible	In process	Initiatives
2023	0	1	0	fifteen*	7
<b>Total modified codes of conduct</b>					<b>1</b>

\* Four codes are transnational in nature, in one of them the AEPD acts as co-reviewer.

5 In the Code of Conduct process, meetings are held with all promoters, in order to clarify issues related to the processing of the Codes.

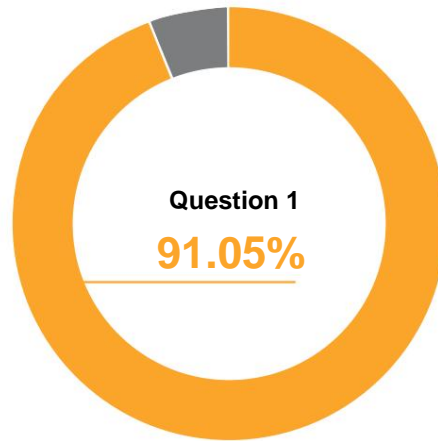
Quality Surveys 2023		
General summary	YEAH	NO
1 Are you satisfied with the content of the information received?	5,527	543
2 Do you consider that the person who assisted you has sufficient technical knowledge?	5,535	535
3 Are you satisfied with the correctness of the treatment by the operator?	5,704	366
<b>Total surveys answered</b>	<b>6,070</b>	
Analysis of responses	YEAH	NO
1 Are you satisfied with the content of the information received?	91.05%	8.95%
2 Do you consider that the person who assisted you has sufficient technical knowledge?	91.19%	8.81%
3 Are you satisfied with the correctness of the treatment by the operator?	93.97%	6.03%
<b>Total surveys answered</b>	<b>100%</b>	
<b>Average satisfaction</b>	<b>92.09%</b>	



### Quality Surveys

Total number 6,070

Are you satisfied with the content of the information received?

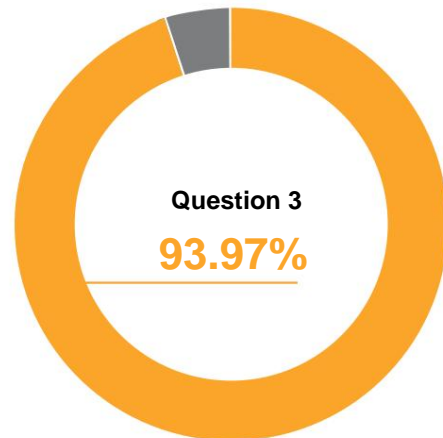
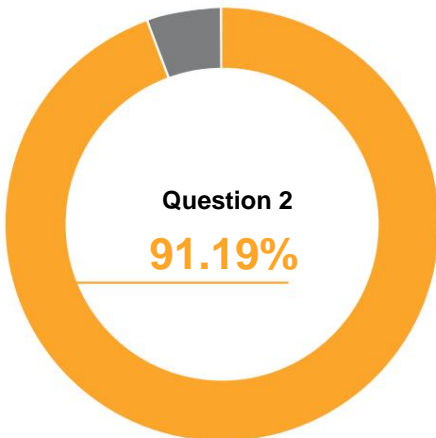


### Quality Surveys

Total number 6,506

Do you consider that the person who assisted you has sufficient technical knowledge?

Are you satisfied with the correctness of the treatment by the operator?

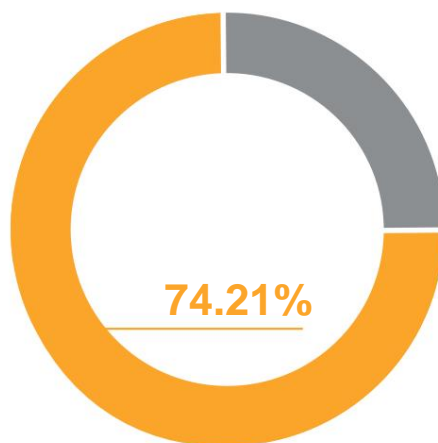


Chatbot Satisfaction Surveys 2023		
<b>General summary</b>	YEAH	NO
1 We want to know your opinion about the service. Have we helped you?	843	293
<b>Total surveys answered</b>	<b>1,136</b>	
<b>Analysis of responses</b>	YEAH	NO
1 We want to know your opinion about the service. Have we helped you?	74.21%	25.79%
<b>Total surveys answered</b>	<b>100%</b>	
<b>Customer Satisfaction Index</b>	<b>74.21%</b>	

**Satisfaction surveys**  
Total number 1,136

Are you satisfied with the content of the information received?

- Yeah
- No



Access to the transparency section			
2021	2022	2023	% 2022-2023
166,290	127,549	173,463	36%

Requests for access to public information <sup>6</sup>					
Year	Applications Granted	Inadmissible <sup>7</sup>	Partially granted	Denied	Withdrawn
2023	112	47	4	4	10

<sup>6</sup> Two applications are currently pending.

<sup>7</sup> Inadmissible includes: Returned to the Central Unit 7 and early terminations (due to accumulation or other causes, 12).

Claims before the CTBG			
Year	Claims	Estimates	Dismissals <sup>8</sup>
2023	9	0	9

<sup>8</sup> Dismissed including Filed 2 and Inadmissible 1.

Register of Data Protection Delegates communicated <sup>9</sup>		Total reported
Ownership		
Private Entities		101,691
Public entities		9,379
	General State Administration	195
	Autonomous communities	457
	Local Entities	4,794
	Other Legal-Public Persons	3,933
	- General Council of the Judiciary	
	- Notaries	
	- Professional Colleges	
	- Universities	
	- Chambers of Commerce	
	- Irrigation Communities	
<b>TOTAL</b>		<b>111,070</b>

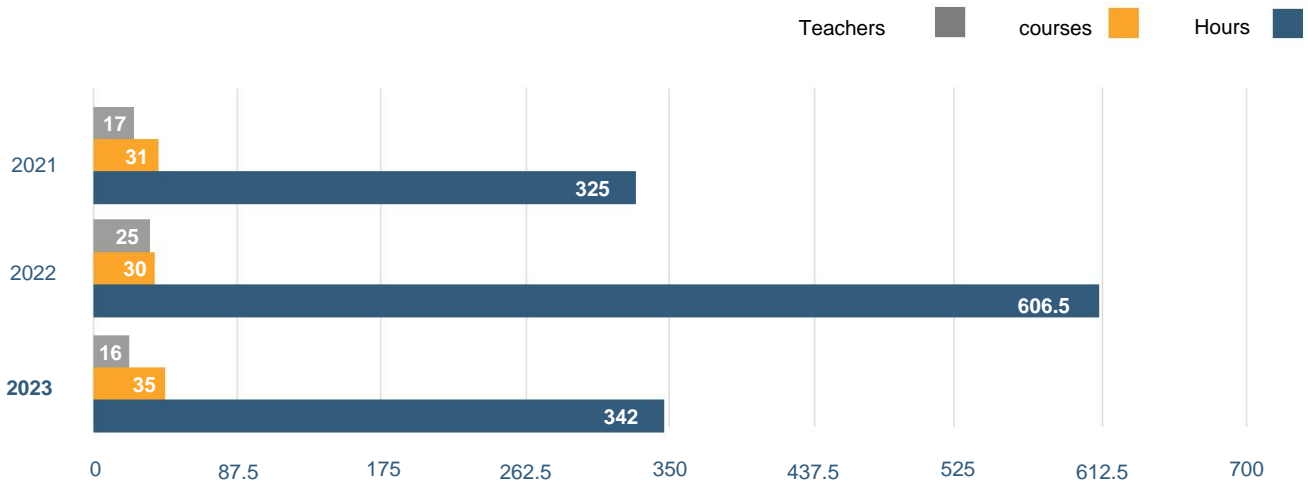
<sup>9</sup> During 2023, 991 queries and incidents related to the communication of DPOs have been answered.

International Transfers since 2019		
	2023	Cumulative total
International transfer authorizations	-	1 (Art. 46.3.b GDPR)
Binding Corporate Rules (BCR) adopted by the AEPD	2	10
Binding Corporate Rules (BCR) being processed by the AEPD as the leading authority	12	-
Binding Corporate Rules (BCR) in which the AEPD has participated as co-reviewer	4	37

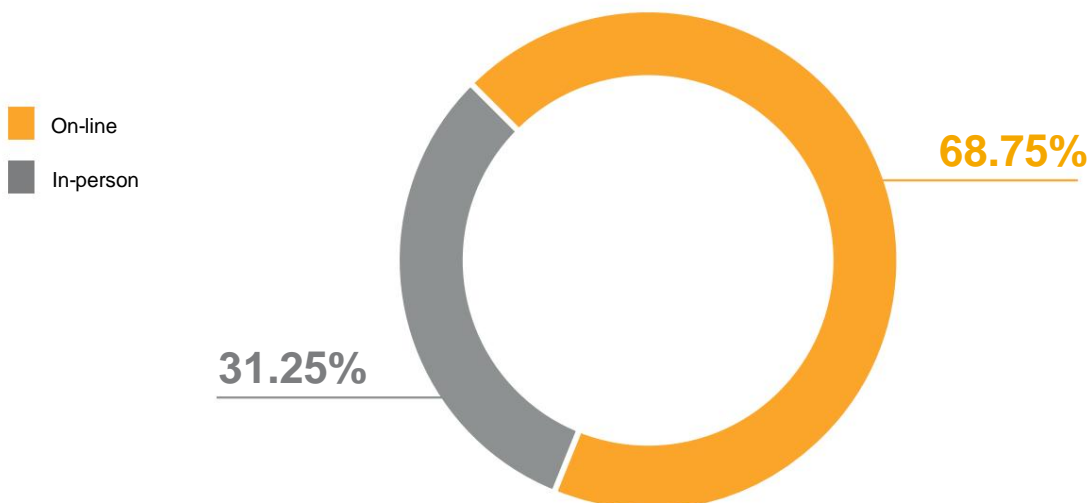
DPD Certification Scheme (AEPD-DPD)			
	2021	2022	2023
Audits	12	4	3
Review of exam questions	8,538	3,932	3,696
Preparation of exams	95	72	78
Monitoring of training entities	164	136	324
Monitoring of certification entities	13	fifteen	14
Recognition of university training	1	1	1
DPD Certificates	175	138	169
<b>Total DPD Certificates:</b>			<b>1,100</b>

Training10			
	2021	2022	2023
<b>courses</b>	17	25	16
<b>Teachers</b>	31	30	35
<b>Hours</b>	325	606.5	342.5

10 Coordinated by the General Subdirectorate of Promotion and Authorizations.



### Course format



The training activities that the AEPD has developed throughout 2023 are detailed below, the management of which has been carried out by the General Subdirectorate of Promotion and Authorizations.

📌 **General Data Protection Courses (online or in-person format)**

Organism	Dates	Duration	Format	No. students
Ministry of Health	02/27 - 03/02	8 p.m.	online	30
Ministry of Social Rights	03/16 - 03/30	10.5 p.m.	online	twenty
Court of Accounts	04/18 - 04/28	8 p.m.	online	60
Las Palmas GC University	05/08 - 05/11	8 p.m.	online	twenty
Ministry of Interior	05/30 - 06/02	8 p.m.	In-person	twenty
Ministry of Education	06/05 - 06/14	8 p.m.	In-person	twenty
Ministry of Labor	06/19 - 06/28	8 p.m.	online	twenty
Ministry of Inclusion	04/07 - 07/07	8 p.m.	In-person	twenty
M. Territorial Policy	09/21 - 10/05	8 p.m.	In-person	30
Ministry of Justice	09/18 - 09/21	8 p.m.	online	twenty
Ministry of Defence	06/10 - 20/10	8 p.m.	online	40
M. Ecological Transition	10/30 - 11/10	8 p.m.	online	30
Ministry of Inclusion	11/21 - 11/24	8 p.m.	In-person	twenty

📌 **General Data Protection Courses (Moodle format), with everything updated the agenda**

Organism	Dates	Duration	No. students
Ministry of Transport	04/24 -06/04	36 hours	30
Ministry of Defence	10/23 - 12/03	36 hours	40

## Conferences and other courses

Organism	Date	Name / Comments
Association of National Experts in Technological Advocacy (ENATIC)	01/25	Privacy Day Webinar. The figure of the DPD.
ISMS Forum	02/16	XV Privacy Forum. "Codes of conduct, certifications, standards and mediation mechanisms to strengthen data protection."
Human Rights and Equality Area of the National Police	02/21	III Human Rights Course, course aimed at Higher Level - commissioners and principal commissioners - National Police. Raise awareness of the new vulnerabilities of Human Rights in ICT.
Diplomatic School	08/03	"Protection of personal data abroad".
Democratic Union of Pensioners and Retirees and the Telefónica Foundation	03/16	II Congress on the Right to Personal Autonomy 'Technology in the daily lives of older people'. Opening conference.
General Directorate for Equality Racial Ethnic Treatment and Diversity Ministry of Equality	03/24	III Antiracist Week. Round table on the specific proposal of the Ministry of Equality to collect data on ethnic origin by the INE in 2026.
Center for Legal Studies	04/05	Data Protection.
Spanish Association of Industrial Pharmacists (AEFI)	06/06	41 AEFI Symposium. Round Table "Code of Conduct regulating the processing of personal data in the field of clinical trials and other clinical investigations and pharmacovigilance."
ENATIC	07/06	Webinar. X-ray of DPD in Spain. Malpractice, professional liability and risks for data controllers.

### 📅 Courses in the educational and minor environment

Organism	Date	Name / Comments
The Family Watch Foundation	March 16	Presentation of the "Guide that does not come with the mobile phone" with the 10 keys that families must have when giving the first mobile phone to their children. Aimed at mental health experts.
Asturian Institute of Administration. Public "Adolfo Posada"	April 18 and 25 online	Data processing in the educational environment. Addressed to Educational Inspection staff.
Digital Classrooms of the Coca-Cola Foundation	April, the 21st	Presentation of the "Guide that does not come with the mobile phone" with the 10 keys that families must have when giving the first mobile phone to their children.
Bar Association of Malaga	may 19	III Family Congress in Malaga, Round Table: "Current challenges in minors and adolescents: Harassment on social networks. Bullying".
AEPD/Spanish Agency for International Cooperation for Development (AECID)	June 28th	Webinar on digitalization and minors.
Valencian generalitat	October 24th	I Congress on data protection in the educational community.
King Juan Carlos University	November 10	I International Congress of Clear Communication. Special attention to vulnerable audiences such as children.
AEPD/INTEF/INCIBE	Nov. 16	MOOC "Educate in security and privacy".

### 📅 Conference on digital violence against women and the Priority Channel

Organism	Date	Name / Comments
Diagram Foundation	09/22	Day on early prevention of gender cyber violence in young people.
Violence Against Women Unit- Subdelegation of the Government in Segovia	07/11	The digital dimension of Violence against women.
Ministry of Justice	11/24	Gender violence day.



ÿ **Courses that are programmed and taught for personnel at the service of the Public Administration to through INAP**

Denomination	Date	No. of students
Specialized program for DPD of the AA.PP.	02/13 to 06/12	80
Application of the RGPD in the AA.PP.	02/20 to 03/24	300
Application of the RGPD in the AA.PP.	09/25 to 10/30	300

ÿ **Courses that are programmed and taught for personnel at the service of the Public Administration to through INAP**

Denomination	Date
Presentation of the Codes of Conduct as an instrument to promote the agile resolution of disputes (telephone operators)	January 17
DPD-EELL Meeting-Provincial capital city councils, with more than 100,000 inhabitants, Provincial Councils, Town Councils and Island Councils	28th March
Conference on Data Protection and Health Research. Impact of technological innovation on the processing of personal data in health research	May 3
Regulatory quality conference in data protection: the advisory role of the Agency in the development of standards and the Report of Regulatory Impact Analysis (MAIN); risk analysis and impact assessments on data protection in regulatory production, the impact of the RGPD on the content of the standards and guarantees to be incorporated into the standard	may 23
Information session with Stetson Law School students University of Florida, on the protection of personal data in the workplace	8 of June
The AEPD and the Platform for Seniors and Pensioners (PMP) organize the Meeting "Seniors in the digital environment"	June 27th

Facilitates GDPR11	
	2023
Access	51,783
Completed questionnaires	20,432
Accumulated	1,109,161



11 Facilitates RGPD, a tool to facilitate compliance with the RGPD for companies and professionals.

Facilitates EMPRENDE12	
	2023
Access	2,746
Completed questionnaires	695
Accumulated	18,700



12 Facilitates EMPRENDE, a tool to help entrepreneurs and technology startups comply with data protection regulations.

MANAGE13 14			
Section	Open	Finished	Accumulated
Privacy Impact Assessments (PIAs)	2,775	967	33,453
Risk analysis	1946	621	31,437



13 Manages EIPD: Assistant for risk analysis and impact assessments in data protection.

<sup>14</sup> These figures from the GESTIONA tool refer exclusively to the period between January 1 and June 14, 2023, when the new version of this tool was published.

MANAGE V215	
	2023
Access	25,369
Number of reports downloaded	937

– The new version of the GESTIONA tool called GESTIONA V2 only allows you to see the number of accesses and number of downloads of the report it performs since the application runs directly on the user's terminal and does not provide any information about the type of process carried out by the user.



Assess RGPD16 Risk		
	2022	2023
Access	101,897	222,463
Accumulated		330,494

16 Evalúa\_Riesgo RGPD: tool whose objective is to help those responsible and in charge to identify the risk factors of personal data processing; make a first, non-exhaustive assessment of the intrinsic risk, including the obligation to carry out a DPIA, and facilitating the management of residual risk by using measures and guarantees to mitigate said risk.



COMUNICA-RGPD17 Gap	
	2023
Access	5,344
Completed questionnaires	993
Accumulated	16,706

17 Communicate-Gap GDPR, a resource so that any organization, responsible for processing personal data, can assess the obligation to inform natural persons affected by a security breach of personal data.



ADVISOR-RGPD18 Gap	
	2023
Access	6,491
Completed questionnaires	1,883
Accumulated	19,736



18 RGPD Gap Advisor, a useful resource for any organization responsible for processing personal data, to assess the obligation to notify the Spanish Data Protection Agency without undue delay of a personal data breach, as established in the article 33 of the General Data Protection Regulation.

ValidaCripto19	
	2023
Access	4,086
Number of reports downloaded	125



19 The ValidaCripto tool was published on October 5, 2023 and, therefore, there is no accumulated value from previous years.

## 4. Technological innovation division

### Personal data breaches (Articles 33 and 34 GDPR)

Personal data breach notifications	2004
Resolutions to force gaps to be communicated to interested parties	30
Transfers to the General Subdirectorate of Data Inspection	16
Number of stakeholders to whom the gaps have been communicated	17,000,000

### Personal data breaches (Articles 33 and 34 GDPR)

Previous inquiries received	3
-----------------------------	---

## 5. International presence of the AEPD

Meeting	Date	Place
<b>Plenary Sessions of the Committee European Data Protection</b>	January 17	Video conference
	February 13 and 14	Brussels, Belgium)
	February 28th 28th March April 13th April 26	Video conference
	May 24 and 25	Brussels, Belgium)
	June 20th July 18 August 2nd	Video conference
	September 19 and 20	Brussels, Belgium)
	October the 17th October 27th	Video conference
	November 14th December 12th	Brussels, Belgium)

### European Data Protection Board subgroup meetings

Meeting	Date	Place
<b>Advisory Subgroup (Strategic advisory)</b>	February 7th	Video conference
	23 of February	
	March 29	
	June 26th	
	July 17th	
	September 5	
	September 12	
	October 16	
	October 19	
	October 24th	
	November 10	
	November 20 December 20th	

European Data Protection Board subgroup meetings		
Meeting	Date	Place
<b>Cookie Banners Working Group</b>	October 11th November 15	Video conference
	January 23 23 of February	Video conference
<b>Digital Social Media (Social media)</b>	may 23	Brussels, Belgium)
	June 29 September 7th October 10th	Video conference
	December 7th	Brussels, Belgium)
	January 18	Video conference
<b>Cooperation</b>	February 9	Brussels, Belgium)
	March 21st April 18th April 24 May 16	Video conference
	June, 15	Brussels, Belgium)
	August 22nd August 30th September 5 September 26 October 19	Video conference
	Nov. 16	Brussels, Belgium)
	January 19 February 20th 6th of March March 13 April 4 May 3 June 6th July 7th July 11	Video conference
<b>Financial affairs</b>		

European Data Protection Board subgroup meetings		
Meeting	Date	Place
<b>Financial affairs</b>	September 9	Brussels, Belgium)
	November 28	Video conference
<b>International transfers</b>	January 10 and 11 January 31 and February 1 Feb. 10	Video conference
	May 31 and June 1	Brussels, Belgium)
	July 4th	Video conference
	September 5 and 6	Brussels, Belgium)
	October 4 and 5 November 7 and 8	Video conference
	December 5 and 6	Brussels, Belgium)
	February 7th	Video conference
<b>Fines Working Group</b>	March 9	Brussels, Belgium)
	April 19th 8 of June September 13th November 15 December 11	Video conference
<b>Working group 101 Schrems II complaints of the CJEU</b>	February 6th 6th of March	Video conference
<b>Borders, Travelers and Legislative Enforcement (BTLE)</b>	26 of January Feb. 10 23 of March May 4th	Video conference
	June, 15	Brussels, Belgium)



European Data Protection Board subgroup meetings		
Meeting	Date	Place
<b>Borders, Travelers and Legislative Enforcement (BTLE)</b>	September 15 October 26th	Video conference
	November 30	Brussels, Belgium)
	January 25	Video conference
<b>Key provisions (Key Provisions)</b>	March 1st	Brussels, Belgium)
	April 18th May 30 July 6th	Video conference
	September 26	Brussels, Belgium)
	October 26th November 21 and 22	Video conference
	February 8th	Brussels, Belgium)
	February 17th March 2 March 16 March 22 April 4 April 18th	Video conference
<b>Compliance Monitoring (Enforcement)</b>	June 7	Brussels, Belgium)
	19th of June June 27th July 4th July 10th July 20th August 22nd August 30th September 12	Video conference
	October 18	Brussels, Belgium)
	December 5th	Video conference

European Data Protection Board subgroup meetings		
Meeting	Date	Place
<b>Users of CEPD information systems (IT Users)</b>	March 13	Brussels, Belgium)
	June 16 October 9 December 4th	Video conference
	January 18 and 19	Video conference
<b>Technology</b>	February 16th	Brussels, Belgium)
	March 22 April 19th May 10	Video conference
	June 14th	Brussels, Belgium)
	July 13 September 13th	Video conference
	October 18 and 19	Brussels, Belgium)
	Nov. 16 December 4th	Video conference
	January 24 February 21st	Brussels, Belgium)
	March 16	Video conference
<b>Compliance, E-government and Health &amp; Health)</b>	April 27 may 17th	Brussels, Belgium)
	8 of June 19th of June June 26th July 11	Video conference
	September 21st	Brussels, Belgium)
	October 20 November 7 Decembre 19th	Video conference

European Data Protection Board subgroup meetings		
Meeting	Date	Place
<b>GPT Chat Working Group</b>	April 18th	Video conference
	May 3	
	12th of July	
	September 6	
	October 20	
	November 8th	
	December 1st	
<b>Competition and Consumption Working Group</b>	28th of April	Video conference
	June 21	Brussels, Belgium)
	September 6	Video conference
	November 15	
November 23		
	December 15	
<b>International Working Group</b>	May 22nd	Video conference
	July 10th	
	September 18	
	November 27	
Control of EU Agencies and Large Information Systems		
<b>Supervision Group CSC Coordinated</b>	March 22	Video conference
	June 14th	Brussels, Belgium)
	September 7th	Video conference
	November 29th	Brussels, Belgium)
<b>Coordinated Supervision Group of SIS II</b>	March 22	Video conference
	June 14th	Brussels, Belgium)
	September 7th	Video conference
	November 29th	Brussels, Belgium)
<b>EUROPOL Coordinated Supervision Group</b>	March 22	Video conference
	June 14th	Brussels, Belgium)
	November 29th	Brussels, Belgium)
<b>Schengen evaluation</b>	October 8 - 15	Riga (Latvia)

Other meetings		
Meeting	Date	Place
Meeting of Mediterranean experts and DPAs	January 26 – 31	(Rabat) Morocco
XX Health Data Security and Protection Forum	February 17 – 16	Palma de Mallorca
	October 5th	Malaga
Mobile World Congress	February 27 – February 1 March	Barcelona
Data Protection and EU Integration	March 14 – 15	Warsaw, Poland)
Privacy Symposium 2023	April 16 – 22	Venice Italy)
Spring Conference	May 9 – 12	Budapest, Hungary)
Agency Coordination Meeting Autonomous PD	May 29 – 30	Barcelona
Berlin Group	June 5 – 7	Rome Italy)
	December 5 – 8	Ottawa (Canada)
Global PETs Regulator Network Conference	June 25 – 28	Tel Aviv (Israel)
Human Rights in Sports Forum (CoE)	June 29 – 30	Paris France)
Personalized Digital Care and the European Health Data Space	September 26 – 30	Lion
Global Privacy Assembly	October 14 – 22	Bermuda (Bermuda)
Meeting of the HLG on access to data for effective law enforcement	October 3 – 4 November 21	Brussels, Belgium)
International regulations regarding Cybersecurity and Personal PD	November 18 – 24	Mexico City (Mexico)
Certification Workshop	November 22 – 24	Luxembourg (Luxembourg)
Octopus Conference 2023	December 13 – 15	Bucharest (Romania)
Meta EU Youth Forum	December 5th	Brussels, Belgium)

Council of Europe		
Meeting	Date	Place
Convention Committee 108 – Table	March 22 – 24	Paris France)
	September 27 – 29	
Convention Committee 108 - Plenary	June 14 – 16	Strasbourg (France)
	November 15 – 17	
Artificial Intelligence Committee	January 11 – 13	Strasbourg (France)
	February 13th	
	April 19 – 21	
	May 31 – June 2	
	October 23 – 26	
	December 5 – 8	Video conference

RIPD Meetings	
Meeting	Number of meetings
RIPD meeting Santa Cruz de la Sierra, Bolivia	1
RIPD XX Anniversary Meeting, La Antigua, Guatemala	1
DPF-RIPD Members Webinar	1
RIPD ChatGPT Joint Action	1
Joint action RIPD IACHR	1
Meetings National Institute of Transparency, Access to Information and protection of Personal Data (INAI)	3
Visit AGETIC Studies (Bolivia)	1
Transparency Institute Meeting, Access to Information Public and Protection of Personal Data of the State of Mexico and Municipalities (INFOEM)	1
Ibero-American General Secretariat Meetings (SEGIB)	3

RIPD Meetings	
Meeting	Number of meetings
EU-funded project collaboration meetings	2
Meeting of the Chilean Financial Market Commission (CMF)	1
Ecuador Telecommunications Ministry Meeting	1
Electronic Government and Information Technologies Agency Meeting Information and Communication (AGETIC), Bolivia	1
IPANDETEC Meeting, Panama	1
California Privacy Agency (CPPA) Meeting	1
Resident Data Protection Agency Meeting (PRODHAB), Costa Rica	2
Meeting Latin American University of Science and Technology, Costa Rica	1
AECID (Spanish Agency for International Cooperation for Development)	6
UNESCO meetings	2
RIPD Executive Committee Meetings	2
Presentations at seminars	3

## 6. General Secretariat

Budget evolution			
	Fiscal Year Credit		
	2021	2022	2023
Chapter I	8,751,570	9,882,840	11,600,400
Chapter II	5,235,310	5,359,840	5,468,240
Chapter III	350,950	350,950	320,950
Chapter IV	475,520	350,990	351,590
Chapter VI	928,350	928,350	998,350
Chapter VIII	20,800	11,200	11,200
<b>TOTAL</b>	<b>15,762,500</b>	<b>16,884,170</b>	<b>18,750,730</b>

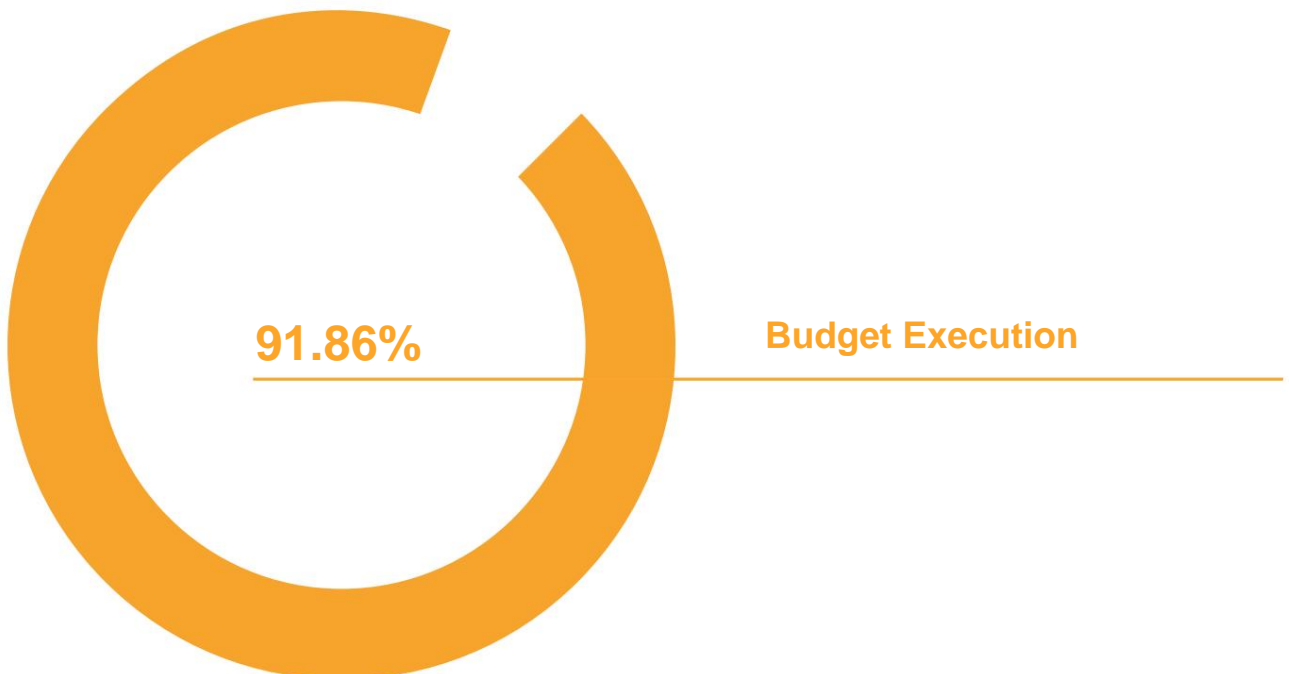
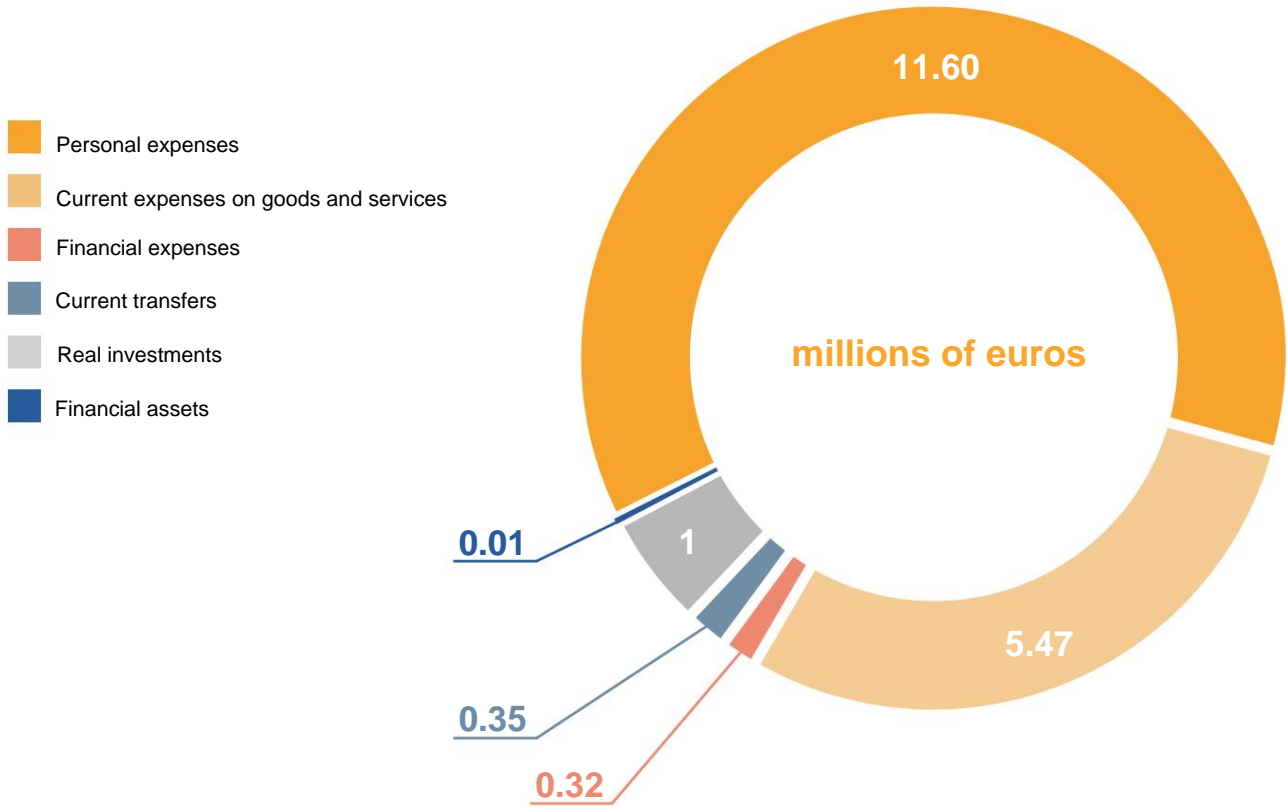
2023			
	Final budget	Recognized obligations	Execution percentage
Personal expenses	11,600,400	10,905,786.54	94.01%
Current expenses on goods and services	5,468,240	5,006,079.32	91.55%
Financial expenses	320,950	1,128.38	0.35%
Current transfers	351,590	349,490	99.40%
Real investments	998,350	1,216,948.08	121.90%
Financial assets	11,200	4,825.80	43.09%
<b>TOTAL</b>	<b>18,750,730</b>	<b>17,484,258.12</b>	<b>93.25%</b>

2022			
	Final budget	Recognized obligations	Execution percentage
Personal expenses	9,882,840.00	9,505,277.87	96.18%
Current expenses on goods and services	5,359,840.00	4,818,377.76	89.90%
Financial expenses	350,950.00	160,954.37	45.86%
Current transfers	350,990.00	347,990.00	99.15%
Real investments	928,350.00	669,939.18	72.16%
Financial assets	11,200.00	6,629.14	59.19%
<b>TOTAL</b>	<b>16,884,170.00</b>	<b>15,509,168.32</b>	<b>91.86%</b>

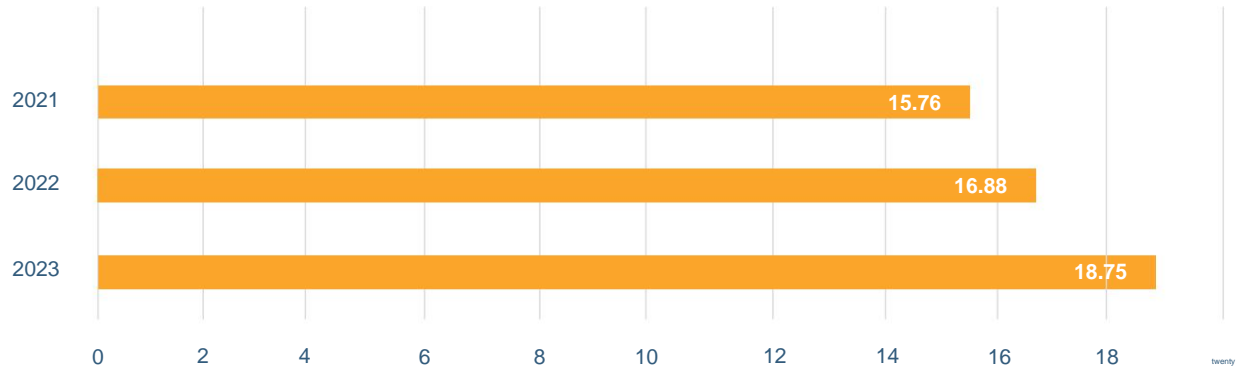
Difference 2023 - 2022		
	Final budget	Recognized obligations
Personal expenses	1,717,560	1,400,508.67
Current expenses on goods and services	108,400	187,701.56
Financial expenses	-30,000	-159,825.99
Current transfers	600	1,500
Real investments	70,000	547,008.90
Financial assets	0	-1,803.34
<b>TOTAL</b>	<b>1,866,560</b>	<b>1,975,089.80</b>



### Budget distribution (in millions of euros)



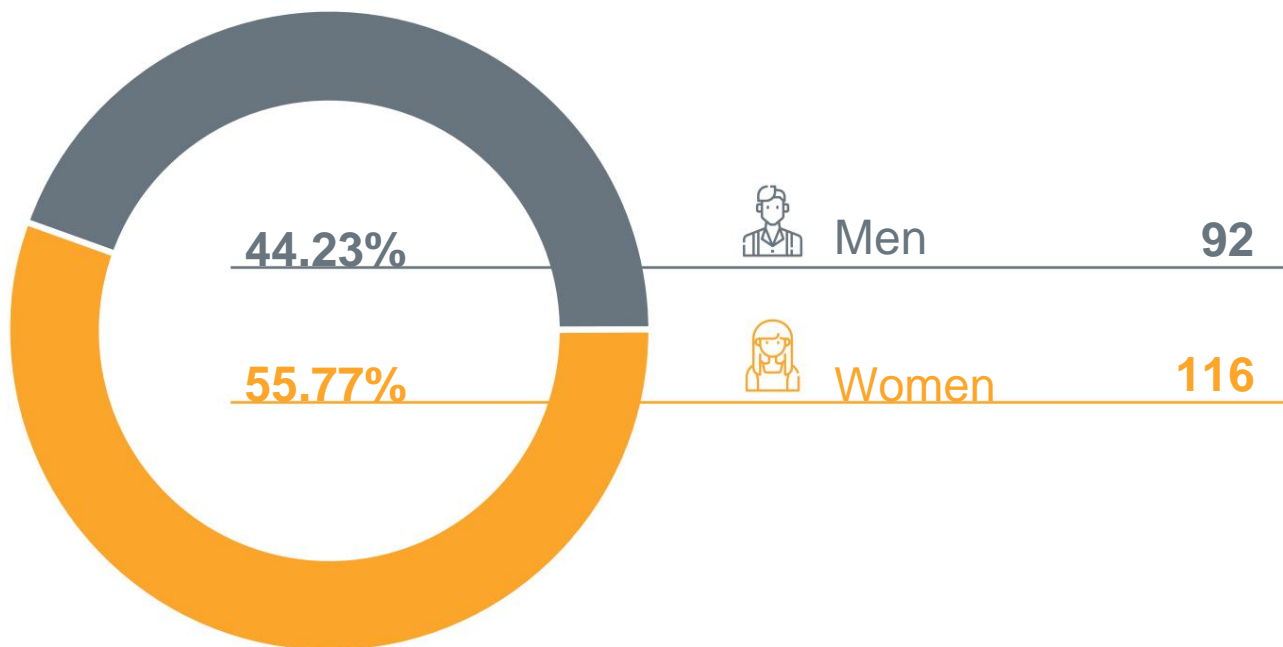
### Evolution of budget credit (millions of euros)



### Human resources management as of December 31, 2023

	Endowment	Covered
<b>Officials</b>	236	198
<b>Labor</b>	8	7
<b>Non-Convention Labor</b>	2	2
<b>Senior</b>	1	1
<b>TOTAL</b>	<b>247</b>	<b>208</b>

The difference between the provision of positions and the effective occupation is due to the fact that civil servant positions include positions reserved for holders who are occupying another job, positions created to be filled through public employment offers, as well as those positions that are in the process of being awarded in the general competition in progress called by Resolution of October 31, 2023.

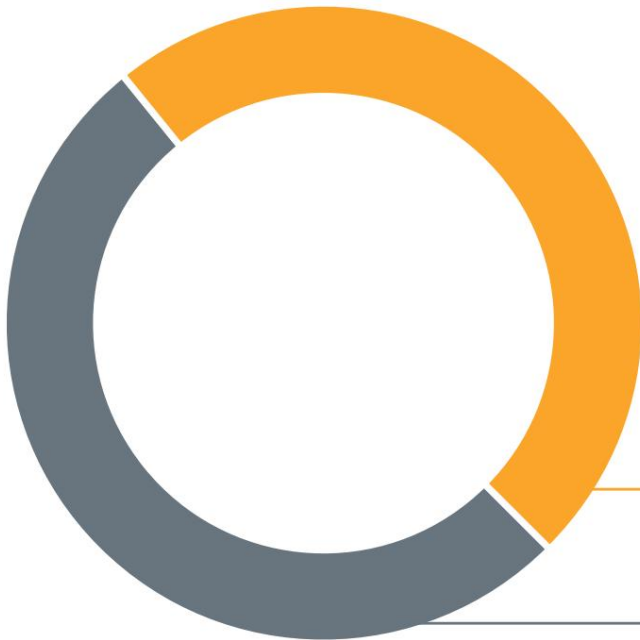


Official staff												
Level	30	29	28	26	24	22	20	18		17	16	14
Effective	eleven	8	46	75	0	30	0	twenty	2	5	1	0

Cluster	A1	A2	b	C1	C2
Effective	69	72	1	35	twenty

Division by levels					
	Level 30	Level 29	Level 28	Level 26	TOTAL
Men	4	6	28	33	71
Women	7	2	18	40	67
TOTAL	eleven	8	46	73	138

### Division by levels



Before the approval of the AEPD Equality Plan in 2020, the Agency had 61.54% men compared to 38.46% women in these positions. As of December 31, 2023, these percentages stand at **51.45% of men compared to 48.55% of women**, that is, in just 4 years the female presence at management levels has increased by 10 points. and pre-directors of the Agency.



Women

67



Men

71

### Evolution of the Civil Servant and Labor Personnel (RPT) workforce

Year	Endowments
2017	180
2018	186
2019	202
2020	202
2021	203
2022	217
2023	246

