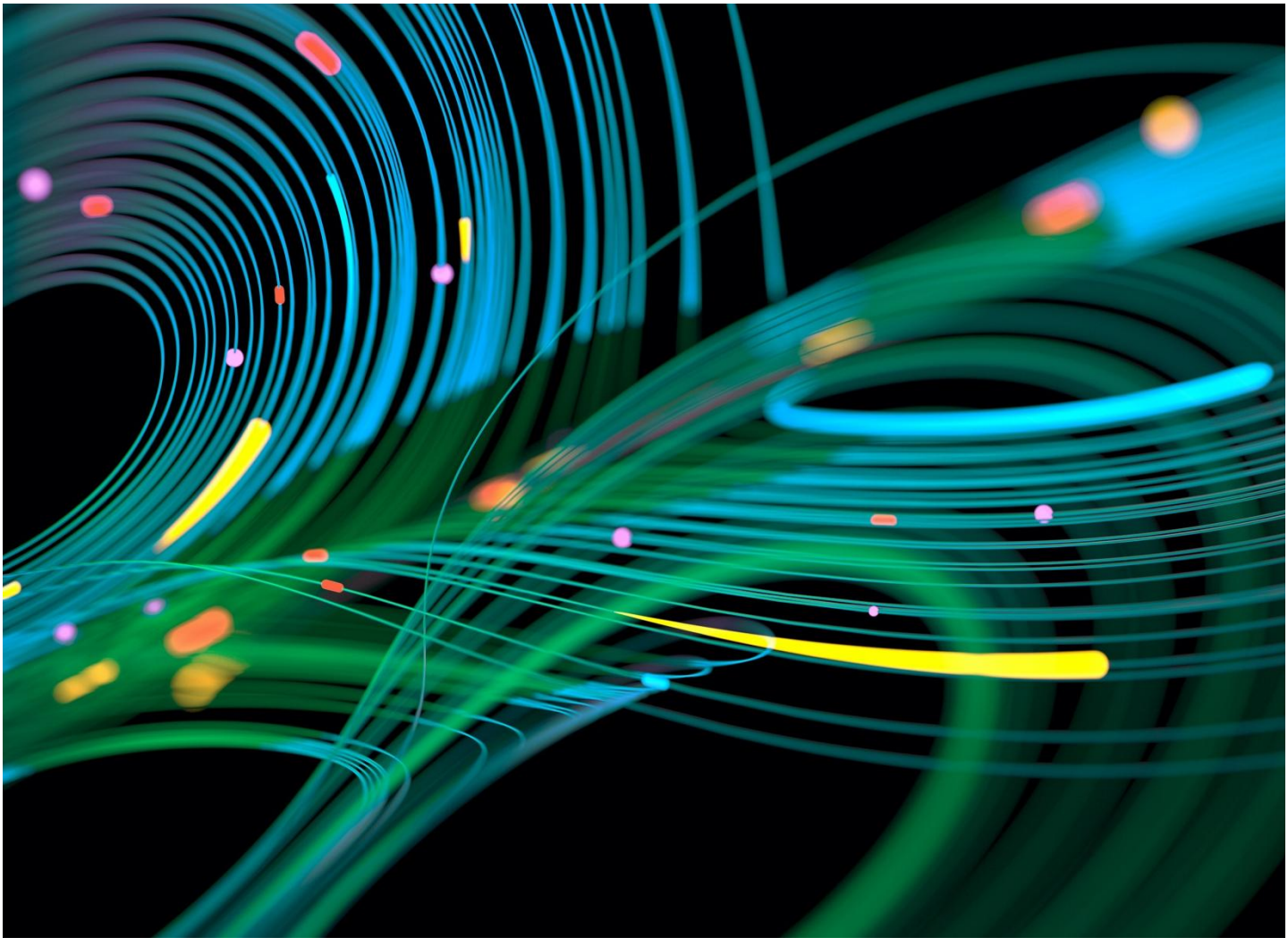
GARRIGUES

Data Economy, Privacy and Cybersecurity Newsletter

April 2026

Latest developments in digital law and technological innovation, featuring recent rulings and key judgments on AI, e-commerce and technology-related legislation



The Supreme Court defines the scope of 'processing' and requires compliance with the GDPR from the moment personal data is requested

Álvaro Blanco and Javier Enebral

The Supreme Court issues a landmark ruling laying down case law in relation to the GDPR: a mere request for personal data constitutes data 'processing' for the purposes of the GDPR. The judgment stems from a cassation appeal brought by the AEPD, with Garrigues acting as legal counsel.

On March 26, 2026, the Judicial Review Chamber of the Supreme Court issued a judgment of particular relevance in the area of personal data protection, marking the first time in Spain that the Court has ruled on the scope of the concept of 'processing' as set out in article 4(2) of the General Data Protection Regulation (GDPR). In this regard, the Supreme Court held that **data controllers are required to comply with the GDPR's data processing principles** – including the principle of data minimization (article 5.1 c) of the GDPR) – **from the moment they request personal data from an individual, regardless of whether such data are ultimately provided** and subsequently collected by the controller.

Background of the case

The case stemmed from a penalty proceeding initiated by the Spanish Data Protection Agency (AEPD) against the Office of the General Secretary of Penitentiary Institutions (SGIIPP). As set out in the facts of the judgement, in 2019 a public official from the Lanzarote Penitentiary Center was absent from work for three days due to health reasons and submitted the appropriate medical certificate, which stated "indisposed." He also justified a subsequent partial absence with proof that he had attended a medical consultation.

After submitting these certificates, management at the Penitentiary asked the public official to provide the specific medical diagnosis and the treatment that had been prescribed. The official refused to do so, arguing that its content was personal and that it was not necessary for him to provide this information. As a result of his refusal, disciplinary measures were imposed on him.

Following the performance of the relevant investigative procedure, the AEPD imposed a penalty on the Office of the General Secretary of Penitentiary Institutions, due to the breach of the principle of data minimization set out in article 5.1.c) of the GDPR, on the grounds that the request for the medical diagnosis was excessive and unnecessary for the purpose of monitoring workplace absenteeism.

National Appellate Court judgment: the restrictive interpretation

The SGIIPP filed an appeal for judicial review at the National Appellate Court against the ruling and the Court issued an initial judgment annulling the AEPD's penalty, based on a formalistic and literal interpretation of article 4.2 of the GDPR. The Court found that there could be no "processing" of personal data where no actual collection of such data had taken place at any point. In its reasoning, the chamber held that since the public official had not actually provided the required data, the authorities were unable to carry out any processing activity and, therefore, the essential element of the infringement relating to the principle of personal data minimization was missing.

The cassation appeal and the matter of cassational interest

The AEPD filed a cassation appeal against the National Appellate Court judgement. As in the previous instance, professionals from Garrigues' Data Economy, Privacy, and Cybersecurity practice acted as legal counsel.

The AEPD's defense argued that the National Appellate Court's interpretation ran counter to case law by the Court of Justice of the European Union (CJEU), citing, inter alia, the judgments of February 24, 2022 (case C-175/20), October 5, 2023 (case C-659/22) and October 4, 2024 (case C-548/21). The thread of argument in the appeal pivoted on the premise that the GDPR requires data controllers to design and implement their procedures in light of the principles laid down in the GDPR on an a priori basis, that is, prior to any physical handling of personal data. Accordingly, compliance with the GDPR – including the principle of data minimization – must occur before the personal data is physically received by the data controller, pursuant to the principles of accountability and privacy by design.

Case law by the Supreme Court

In the judgment in question, the Supreme Court quashed and set aside the National Appellate Court's judgment on the grounds set out below and establishing the following case law:

- **Broad and systematic interpretation of article 4.2 of the GDPR.** The chamber rejected the literal and formalistic interpretation that made the existence of 'processing' dependent on the actual collection of the data. Instead it carried out a systematic interpretation linking the definition set out in article 4.2, with the obligations incumbent on the data controller under articles 5 and 25 of the GDPR. The Court concluded that data 'processing' takes place as soon as the authorities ask an individual to provide personal data, even where the data are not ultimately provided, in light of the numerus apertus nature of the list of activities described in article 4.2 of the GDPR as constituting data processing.

- **Effective protection of fundamental rights.** The Supreme Court underscored that the effective protection enshrined in article 8.1 of the Charter of Fundamental Rights of the European Union and article 18 of the Spanish Constitution is only possible if the data processing is deemed to begin when the request to provide personal data is made. Making compliance with the principles conditional upon the actual "physical receipt" of the data would hinder effective protection of data subjects' rights and would create uncertainty incompatible with the principle of legal certainty.

- **Alignment with CJEU case law**. The Supreme Court judgment is expressly in line with CJEU case law. Indeed, in its judgment of February 24, 2022 (case C-175/20) the CJEU had already held that the EU legislature had intended to give the concept of 'processing' a broad scope, indicating that a request for personal data by the authorities initiates a process of 'collection' of those data, within

the meaning of article 4.2 of the GDPR. The court also cited the CJEU judgement of October 5, 2023 (case C-659/22), which reiterated this broad interpretation.

Application to the case in question: breach of the data minimization principle

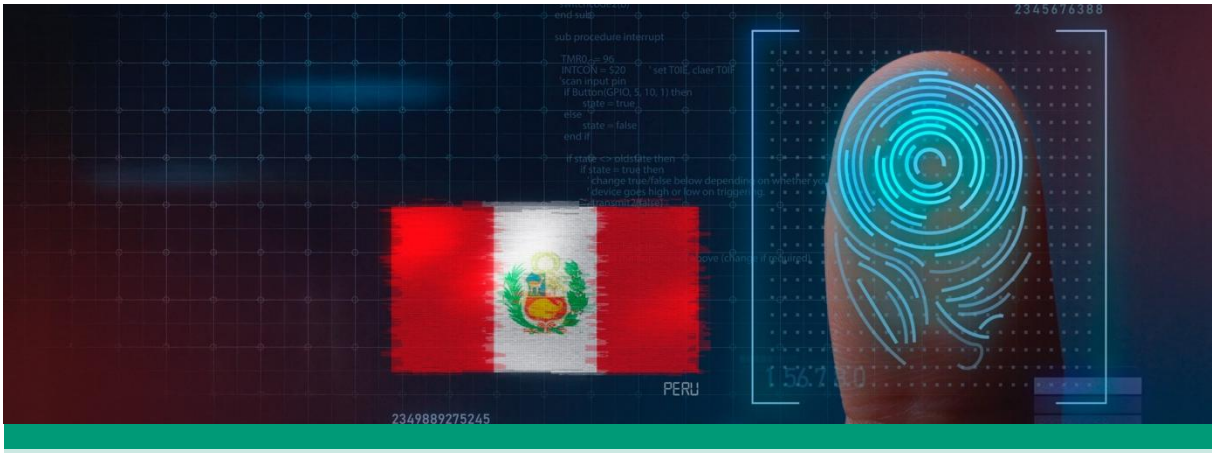
In the case at issue, the chamber held that the Lanzarote Penitentiary had **breached the data minimization principle by requesting the public official's medical diagnosis, since this information was neither appropriate, pertinent or necessary for the purpose of monitoring workplace absenteeism**, which could be adequately carried out using the medical certificates that had already been provided The Court underscored that the information requested constituted specially protected health data and that even where an employee is formally on sick leave, the employer does not – and should not – have access to the worker's medical diagnosis, since both the National Social Security Institute (INSS) and the General Mutual Insurance Scheme for State Civil Servants (MUFACE) expressly exclude this information from the reports provided to employers.

The far-reaching importance of the criterion established

This judgment constitutes a milestone in the interpretation of the GDPR in Spain for several reasons. First, because the Supreme Court has set out, for the first time, its case law position on the scope of the concept of personal data 'processing', extending it to stages as early as the actual request for such data – an issue that had not previously been addressed in a cassation appeal. Second, because it brings Spanish case law into line with the approach adopted by the CJEU since 2022 in the aforementioned judgments, reinforcing the overall coherence of the European data protection system. Third, because it has a profound practical impact: any entity, whether public or private, that acts as data controller must assess compliance with the GDPR principles, especially data minimization, before requesting any personal data, rather than only after such data have been effectively collected.

The criterion established by the Supreme Court strengthens the preventive and proactive approach that underpins the GDPR, reinforcing the principle of accountability and data protection by design and by default. Consequently, organizations are required to design their data collection processes in accordance with the principles of the Regulation before carrying out any processing activities.

Evolution of person data rules in Peru: Implementation of the new regulations, administrative action and legislation forecasts



Franco Muschi and Mariana Ubidia

Data protection rules have evolved at a particularly vigorous pace over recent years in Peru, fueled by a strengthened regulatory framework (driven by the entry into force of the new Regulations for the Data Protection Law) and increasingly active and technical oversight by the Peruvian data protection authority. These measures are aimed at consolidating and modernizing the protection system, by reaffirming the constitutional protection afforded to personal data in Peru. The result has been a regulatory environment that requires public and private entities to process data more responsibly and with greater security, in alignment with current international standards.

Some of the most significant developments in this area are described below.

Current regulatory framework

Publication of the new data protection regulations

The new Regulations for the Data Protection Law were published on November 30, 2024 (Supreme Decree No 016-2024-JUS). After coming into force on March 30, 2025, they repealed the previous regulations, which had been in effect since 2013. The main new changes they have brought are described below.

1. **Notification of security incidents**

   The regulations require the Data Protection Authority to be notified within 48 hours of becoming aware of a security incident. Additionally, if the incident has a direct effect on the data subject, that data subject must also be notified within the same time limit.

   If the incident has been resolved and/or addressed internally without any impact on personal data, only the Data Protection Authority has to be notified.

The National Digital Security Unit must also be notified where the security incident occurs in and/or through the digital environment.

This obligation is highly important as shown by the fact that in the first half of 2025, more than 748 million cyberattack attempts were recorded nationwide.

2. **Appointment of a data protection officer**

A data protection officer must be appointed at public or private entities handling large volumes of personal data, which may impact a significant number of people, or engaging in primary activities or activities related to their business that imply the processing of sensitive data.

This appointment must be recorded internally in a board resolution and must be reported to the Data Protection Authority. Additionally, the contact information for the data protection officer must be posted in a visible place for data subjects at the company.

Moreover, as of the end of 2025, the Data Protection Authority has issued provisions governing the appointment of the Data Protection Officer, including the legal requirements that the Data Protection Officer must meet in relation to their profile, experience, and training, as well as other important details for determining implementation of this obligation.

The Authority has granted a grace period for compliance with these new provisions until June 2026.

3. **Simplification of the Personal Data Bank Register**

The process for registering, modifying, or canceling personal data banks with the Data Protection Authority's registry has been simplified. It has now become an automatic approval procedure subject to subsequent review.

Publication of methodology for calculating data protection fines

The **methodology used to calculate data protection fines** was published on December 31, 2025. The aim was to provide a clear and objective method for calculating fines for breaches of data protection rules, because the ranges in use involve broad intervals that hinder objective determination. Below are some examples of modifications based on the new breaches included in the new regulations:

Infringement	Amount proposed by the draft
Failure to report cross-border data flows.	1.08 UIT
Processing personal data in violation of established security measures, causing adverse effects on the data subject, or exposing their data without their authorization.	7.50 – 37.50 UIT
Processing sensitive personal data in violation of established security measures, causing adverse effects on the data subject or exposing their data without their authorization.	73.33 UIT

The following amendments were also established:

Calculation methodology published in 2020	Proposed calculation methodology
A 20% aggravating factor will be applied to anyone who commits an infringing act that poses a risk or causes harm to more than **two individuals or a group** of individuals.	A 20% aggravating factor will be applied to anyone who commits an infringing act that poses a risk or causes harm to more than **one** individual or a group of individuals.
A 30% mitigating factor will be applied to anyone who makes an express, written acknowledgment of liability for the accusations, **after being notified of the initiation of an enforcement proceeding.**	A 30% mitigating factor will be applied to anyone who makes an express, written acknowledgment of liability for the accusations **prior to the final investigative report.**

Actions by the Data Protection Authority: what 2025 left us

Fines and trends in the reviewed sectors

According to the Data Protection Authority, the year saw an increase in the number of fines issued for handling personal information incorrectly. The main figures as of the end of 2025 are set out below:

- fines for breaches of the rules in force: 11.3 million soles.
- Number of public and private entities reviewed, mainly in financial and telecommunications: 760.
- Inspection visits nationwide: 198.
- New administrative enforcement proceedings: 136.
- Administrative decisions at first and second instance: 211.

Landmark rulings: guidelines issued by the Data Protection Authority

The advisory opinions issued by the Data Protection Authority constitute technical and non-binding rulings that interpret and clarify the scope of the Data Protection Law and its regulations and provide guidelines to assist public and private entities in fulfilling their obligations. The three most important guidelines issued by the Data Protection Authority are described below:

Who is the data controller in public services operated under concession? (Advisory opinion no 001-2026-DGTAIPD, February 2026)

It confirmed that the concession holder, as the party determining the purposes, means, and security measures of the processing, is the data controller for the personal data of users in the public services provided by this concession holder. In this connection, any third party engaged to provide specific services (e.g., video surveillance or support services) acts as processor or, if subcontracted by the controller, as subprocessor.

It clarified further that any provision of data constitutes a transfer, which is only valid if expressly authorized by the data subject, and the purpose, time limits, and obligations must be documented in an agreement, as well as any security and traceability measures that prevent use or sub-transfers for purposes other than those specified.

Can the board meetings of a legal entity be recorded? (Advisory opinion no 037-2025-JUS/DGTAIPD, September 2025)

This Opinion establishes that a person's voice is considered an item of personal data that must be analyzed from two perspectives: (i) the information transmitted using their voice, and (ii) the physical characteristics associated with the data subject. If audio recordings of the board meetings of a legal entity are covered by the entity's bylaws, it is not necessary to obtain the consent of their participants (directors) to record those meetings, provided that matters related to the legal entity are being discussed, because the individual would be acting on the entity's behalf.

Once the purpose of recording a board meeting has been fulfilled, any subsequent processing of the recorded data comes within the scope of the Data Protection Law, because it falls outside the original purpose of representing the entity. The data subject has the right to object to the processing and to request deletion of their data, which will require a specific assessment of each case by the relevant administrative authority.

How should the accuracy of personal data be ensured in the processing of employment information? (Advisory Opinion no 013-2025-JUS/DGTAIPD, March 2025)

The Opinion establishes that any data contained in publicly accessible sources must be used exclusively for the purposes for which they were created and made available. If the data needs to be used for other purposes, the data subject's consent must be obtained. Employers or potential employers can use public information, such as news reports or public registers, to verify the accuracy of data provided by applicants or employees without requiring their consent, provided they comply with the principles of the Data Protection Law.

It also reaffirmed that only the authorities with legal powers can process personal data related to criminal or administrative offenses. Any other person or entity wishing to access such information must obtain the data subject's prior, freely given, and informed consent. In the case of criminal, police, or court records, the information must be requested directly from the data subject.

Agenda for 2026

Case in focus

The start of 2026 has confirmed that the banking and financial sector will always be a primary target for the Data Protection Authority.

At the beginning of the year three banks were fined for obtaining, storing and using fingerprints and biometric data from customers and non-customers without their consent and without prior notification. It was found that these institutions, despite having access to the biometric verification service of the Identification and Civil Registry (RENIEC), were also storing biometric data on their own databases.

In the first case, a 24.75 UIT fine (S/ 122,512.50) was imposed on a financial institution for storing the fingerprints of an individual with no contractual relationship with the institution, who had simply visited to make a deposit. Although the institution used the registry's biometric verification service, it also stored the fingerprints on its own systems. The fine was upheld on appeal.

In the second case, another bank was fined 66 UIT (S/ 326,700.00) after it was found to be collecting fingerprints from both customers and non-customers under the pretext of validation with the Identification and Civil Registry, although they stored the biometric data for additional purposes not disclosed to the individuals concerned.

In both cases, additional fines of 4.89 UIT and 13.50 UIT, respectively, were imposed for failing to have clear, comprehensive, and pre-established privacy policies on the processing of biometric data.

Finally, another financial institution was fined 7.5 UIT (S/ 37,125.00) for deficiencies in security measures that compromised the confidentiality and integrity of users' biometric information.

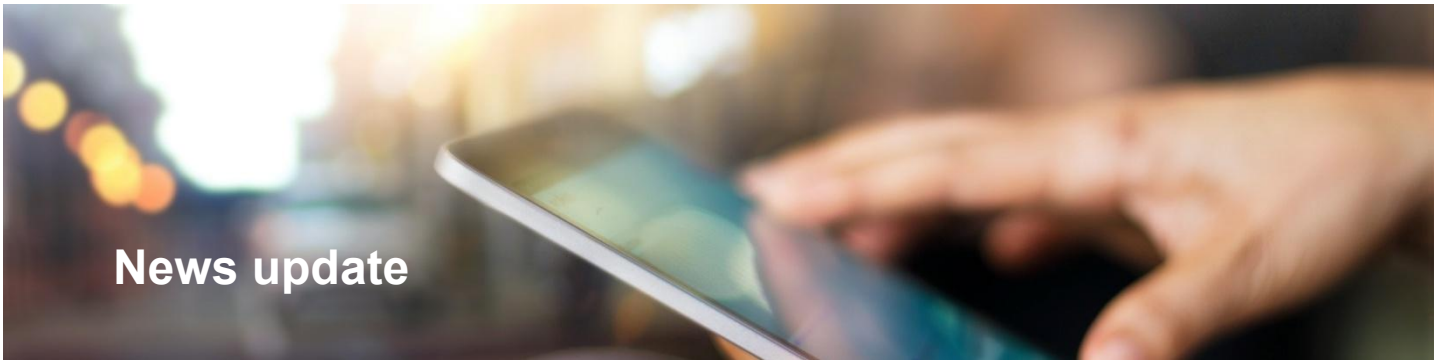
Personal data at public authorities in 2026: Data Governance Strategy

In light of ongoing digitization and digital transformation, a Data Governance Strategy (ENGD) has been proposed, which aims to enhance the management of public data in Peru by promoting efficient, accessible, and secure use of data by public authorities.

This strategy focuses on data governance and the creation of interconnected platforms, such as DATOS PERÚ, the National Data Center, and the National Open Data Platform, to facilitate the exchange of information among public entities. It further promotes the use of technologies, such as data analytics and AI, to optimize decision-making and provide better services.

This strategy engages the private sector by promoting an economic reuse of public data, fostering innovation challenges and business support programs, and ensuring access to standardized data. Moreover, it proposes interoperability aligned with OECD standards, which facilitates secure exchanges between the government and businesses. ¡

Also, the strategy calls for the creation of secure data environments where the private sector participates alongside the government through interoperability and security services. It also requires regular consultation with companies to guide open data plans and support private initiatives that use public data to address public policy issues.



News update

Joint opinion of the European Data Protection Board and European Data Protection Supervisor on proposal for a Digital Omnibus Regulation for simplification of the European regulatory framework

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have issued a joint opinion in response to the proposal for a regulation known as the "Digital Omnibus" proposal, presented by the European Commission on November 19, 2025. This legislative proposal aims to amend a broad set of European Union digital instruments, including the GDPR, the ePrivacy Directive, the Data Act, and NIS 2, all with the goal of simplifying the European Union's digital regulatory framework, reducing the administrative burden, and improving the competitiveness of European organizations.

In their joint opinion, the EDPB and the EDPS assess whether the proposal (i) leads to genuine simplification and facilitates regulatory compliance, (ii) provides greater legal certainty, and (iii) affects individuals' fundamental rights.

The document is set out in sections analyzing the proposed amendments in relation to each affected legislative provision, and specific recommendations are made on each subject. Although the EDPB and the EDPS welcome the simplification goals sought by the Digital Omnibus proposal, they advise of the need to ensure that those simplifications do not undermine the high level of protection of individuals' fundamental rights and freedoms, and regret also that the proposal was not accompanied by a complete impact assessment.

Among the most significant amendments contained in the Digital Omnibus and addressed in the opinion are an amendment to the definition of personal data (in relation to which both authorities express serious reservations), the introduction of a definition of scientific research, new exceptions for the processing of biometric data, the use of legitimate interest in the context of artificial intelligence, amendments regarding data subjects' rights (access, transparency, and automated decision-making), the rules on data breach notifications, data protection impact assessments, the protection of terminal equipment and cookies, and various provisions concerning data governance and reuse.

Spanish government approves preliminary bill for new Organic Law on the right to honor, personal and family privacy, and own image

The Council of Ministers has approved the wording of the preliminary bill for the Organic Law on the civil protection of the right to honor, personal and family privacy, and own image. This preliminary bill replaces the original wording from 1982, adapting it to the digital environment (AI, social media, and so on) and increases the level of protection of these fundamental rights.

The proposed wording toughens the rules on protection against unauthorized use of images, voice and other identifying elements, and addresses emerging factors such as deepfakes. The preliminary bill also clarifies, in its preamble, that the fact of a citizen sharing their own photographs or videos on a social media platform does not authorize third parties to reuse them on other channels or platforms.

The legislation also expands protection for particularly vulnerable groups. In the case of minors, the minimum age for giving valid consent regarding the use of their image is set at 16, although even with consent, such use will be considered unlawful if its dissemination undermines their dignity or reputation. Protection for victims of crimes has also been strengthened, by prohibiting perpetrators from using the facts of the crime to the detriment of the victim. The wording further provides an option for individuals to leave instructions to prevent the use of their image or voice for commercial purposes after their death.

It retains the exceptions that have already been granted in the current version of the legislation or by case law, particularly in relation to freedom of expression and information. These exceptions notably include the ability to use artificial intelligence techniques for creative, satirical, or fictional purposes where they involve public figures, provided that the use of this technology is clearly identified.

Public consultation on the implementation regulations for the legal framework on cybersecurity in Portugal

The National Cybersecurity Centre ("CNCS"), which is the Portuguese cybersecurity authority, has published the bill for the implementing regulations for Decree-Law No. 125/2025, of December 4, 2025, approving the legal framework for cybersecurity ("RJC") and transposing Directive (EU) 2022/2555 ("NIS 2") into Portuguese law.

The regulations are applicable to essential entities, important entities and relevant public entities, under the terms defined in the RJC, and fill out the obligations already provided for in that legal instrument, establishing operational rules and concrete compliance instruments.

The main aspects of the draft regulations are highlighted below:

Electronic platform

A central axis of the regulations is the creation of an electronic platform managed by the CNCS, which will function as a single point of registration, qualification and communication between the entities covered and the cybersecurity authorities. This platform will be the mandatory channel for the fulfillment of several obligations provided for in the RJC, namely: the self-identification and registration of entities; notification of the qualification of entities; the communication of the annual report; the designation of the cybersecurity officer and the permanent contact point; the notification of cybersecurity incidents and the voluntary notification of relevant information; and electronic notifications made by cybersecurity authorities to entities.

National cybersecurity reference framework

The National Cybersecurity Reference Framework ("QNRCS"), set out in Annex I to the draft regulations, is the national reference tool for the identification of rules, standards and best practices in cybersecurity and information security management. According to article 14(3) of the RJC, it will be the reference instrument for determining the cybersecurity measures to be adopted by the covered entities.

It should be noted that the QNRCS and the Risk Matrix (Annex II) are not subject to public consultation, so the contributions of interested parties will be limited to the articles of the regulations and the measures contained in Annexes III and IV.

Risk matrix and minimum cybersecurity measures

The regulations define minimum cybersecurity measures, associated with three levels of compliance - "Basic", "Substantial" and "High" - determined by a sectoral risk matrix. The Risk Matrix, contained in Annex II, considers, for each sector and subsector, the probability and impact of dominant risk scenarios, taking into account the size of the entity ("Large", "Medium" or "Small") and the importance of the sector (critical sectors of Annex I to the RJC or other critical sectors of Annex II to the same legal instrument).

The compliance levels are cumulative, so entities subject to the "High" level must also comply with the measures provided for the "Basic" and "Substantial" levels. The minimum cybersecurity measures are filled out in Annex III (applicable to essential and important entities) and Annex IV (applicable to relevant public entities, organized in Group A and Group

B), covering areas such as cybersecurity policies, asset inventory, risk and vulnerability management, access management and multi-factor authentication, equipment and network protection, backups, incident response, and supply chain management.

Next steps and practical implications

The draft regulation was open for public consultation until April 16, 2026, except for the provisions relating to the QNRCS (Annex I) and the risk matrix (Annex II). The CNCS is currently in the process of assessing the contributions received, and will subsequently publish a report summarizing those contributions, together with an overall assessment of them and the rationale for the options adopted in the final version of the regulations.

The regulations will enter into force on the fifth day after their publication, without prejudice to the transitional provisions provided for in Decree-Law No. 125/2025.

The RJC Implementing Regulations are a key tool for implementation of the cybersecurity mandatory framework. The entities covered must, from now on, start an analysis of the applicable requirements and prepare their respective internal processes, taking into account that some obligations will have short compliance periods after the platform has been brought into operation - namely, the self-identification of entities, which must occur within 60 days.

AEPD publishes guide on use of third-party images in artificial intelligence systems and the related risks

This document analyzes the risks involved in uploading, transforming, or generating content with AI, using images of people, which can be divided into visible and invisible risks. The guide is particularly useful for conducting risk assessments of artificial intelligence systems that process third-party images.

Visible risks are identified as those arising when the generated or modified content is shared. Key factors include the reasonable expectation of the person portrayed regarding its use, the ease of dissemination on social media or messaging platforms, the practical difficulty of removing copies, and the potential reputational damage where the image attributes events that never occurred. It specifically highlights the high risk associated with the generation of intimate or sexualized content, the decontextualization of images, and the use of images of vulnerable individuals, including minors, the elderly, or people with disabilities.

Secondly, the AEPD describes the less visible risks, which arise simply from uploading an image to an artificial intelligence system. Among the many examples are a loss of control over the file, the involvement of multiple technological actors, a chance of the provider using the images for additional purposes, or automatic generation of metadata. It also warns of the risk of persistent identification, information asymmetry that hinders the ability to exercise rights, and potential exposure to security incidents.

General Council of the Spanish Judiciary approves a direction on the use of artificial intelligence by judges

On January 28, 2026, the Plenary Session of the General Council of the Spanish Judiciary (CGPJ) approved Direction 2/2026 on the use of artificial intelligence systems in exercising judicial functions., published in the Official State Gazette (BOE) on January 30, 2026. Its objective is to establish criteria, guidelines, and principles for the use of artificial intelligence (AI) systems by judges as a support tool, to protect judicial independence and fundamental rights, in line with Regulation (EU) 2024/1689 on Artificial Intelligence (the AI Act).

The direction sets out nine principles: effective human control, no substitution of judges, full judicial accountability, judicial independence, respect for fundamental rights, confidentiality and security, prevention of algorithmic bias, and proportionality and continuous training. The use of AI is permitted for legal research, document analysis, and document classification, the preparation of outlines or internal drafts, and organizational tasks. It is prohibited, however, to use AI to replace judicial decision-making, incorporate content without critical validation, or process specially protected data other than in the cases allowed by the law. Only systems provided by the competent authorities or the

CGPJ can be used; external systems are prohibited except for research using open-source data.

Draft decisions generated by AI require review and critical validation by a judge before being validated as a judicial or procedural ruling, and do not constitute automated decisions.

The CGPJ will oversee the use of these systems regarding the processing of personal data for judicial purposes and will provide specialized training. Failure to comply with this direction may result in liability under Organic Law 6/1985 of July 1, 1985 on the Judiciary.

The Transparency and Data Protection Board for Andalucía analyzes an AI system for recruitment

The Transparency and Data Protection Board for Andalucía has published a technical document analyzing the use of artificial intelligence systems for assessing professional competence in recruitment processes, particularly in the public sector.

The report addresses, from a practical perspective, the main implications of using automated tools to evaluate candidates, focusing on issues such as determining the legal basis for data processing, how to apply article 22 of the GDPR regarding automated individual decision-making, and the need to conduct a data protection impact assessment (DPIA) where the system may pose high risks to applicants' rights and freedoms.

The document underscores that, where the AI system plays a decisive role in the pre-selection or ranking of candidates, this may qualify as an automated decision with legal or substantially similar effects, which requires additional safeguards, including the right to human intervention and the right to challenge the decision. It also analyzes transparency requirements, data minimization, and anonymization or pseudonymization techniques that could be applied in the early stages of the process.

The board also emphasizes the need to adequately document how the algorithm works and to ensure that no discriminatory bias occurs, noting that proactive accountability requires evidence of compliance before the system is launched.

European Data Protection Board warns European Commission that new proposals to modify the ESTA system entail collection of a disproportionate amount of data from European travelers

The European Data Protection Board (EDPB) has sent a letter to the European Commission expressing its concern over US proposals to modify the application process for the Electronic System for Travel Authorization (ESTA), which allows citizens of the European Economic Area to enter the United States without a visa for stays of less than 90 days.

According to the EDPB, the proposed changes represent a substantial and problematic shift in the processing of EEA citizens' personal data, as they involve the collection of a significantly larger volume of information, including particularly sensitive data such as social media activity over the past five years, information about family members unrelated to the trip, and even, potentially, biometric data. The board emphasizes that this expansion lacks proportionality and does not meet a demonstrated need.

It further draws attention to the fact that the intention to require applications to be submitted solely via the ESTA mobile application reduces accessibility and raises doubts over the transparency and security of the system, especially as no effective mechanisms for interested parties to exercise their data protection rights are described. And it is also highlighted that the duration of retention or the terms under which the data will be stored or used are not clarified, which exacerbates the lack of safeguards available for European citizens and creates uncertainty over respect for their fundamental rights arising from these proposals.

EDPB publishes results of public consultation on templates to facilitate organizations' compliance with the GDPR

The European Data Protection Board has published a report on the results of the public consultation launched between November 5 and December 3 2025, in which it sought opinions on which templates could facilitate compliance with the GDPR for organizations. The consultation, which was targeted particularly at SMEs and tied in with the undertakings given in the Helsinki Statement on enhanced clarity, support, and engagement, received a total of 82 contributions from business associations, data protection officers, lawyers, companies, public authorities, NGOs, academic institutions, and individuals, of which 71 came from the EEA and 11 from third countries. The templates most requested by contributors were those related to the record of processing activities (RPA), the data protection impact assessment, the legitimate interest assessment, the privacy notice or policy, the transfer impact assessment, the data processing agreement, the data breach notification form, and the privacy risk assessment.

In light of the contributions received, and considering that the EDPB had already decided to work on templates for data protection impact assessments and data breach notifications, the board has included in its 2026–2027 Work Program the creation of three additional templates: a template or flowchart for the assessment of legitimate interests, one for the record of processing activities, and another for privacy notices or policies. In creating these, the EDPB will take into consideration the existing ones at national level and harmonize them. They may also consider working on additional templates.

First regulations approved on use of AI in the Spanish parliament

On February 16, 2026 the Upper House of the Spanish Parliament approved Guidelines on the Use of AI in the Upper House, setting out a framework for responsible, ethical and legal use of AI. Their purpose is to enhance parliamentary and administrative efficiency, while safeguarding rights and freedoms. They are aligned with Regulation (EU) 2024/1689 on artificial intelligence, the GDPR and the Spanish Data Protection Law, and they apply to members of the upper house, staff, parliamentary groups and trainees. Risks to fundamental rights (privacy, bias, intellectual property), and operational, security, reputational and environmental risks are identified.

The prescribed principles of conduct include individual responsibility in use; reliability, robustness, and security of systems; respect for human autonomy; transparency; proportionality and alignment with the Upper House's needs; mandatory human supervision; accountability, including that of the provider where applicable; openness and interoperability; privacy; equality and non-discrimination; and openness to technological advancement.

In relation to the procurement and deployment of AI systems, the guidelines primarily require: (i) a prior assessment supervised by the Upper House's Information Security Committee, (ii) an impact assessment where relevant, (iii) detailed technical documentation, and (iv) a guarantee from the system provider that information entered into the system that is not publicly available will not be used to train any model.

The Information and Communication Technologies Manager is responsible for compliance, in coordination with the data protection officer. There are disciplinary rules for cases of non-compliance. The guidelines come into force 60 after they are published in the Official State Gazette and they set out a six-month adaptation period.

European Commission opens two proceedings to assist Google in complying with interoperability and data-sharing obligations under the Digital Markets Act

The European Commission has opened two proceedings aimed at clarifying how Google, a designated gatekeeper under the Digital Markets Act, has to adapt to the act. This act sets out specific obligations for platforms acting as essential intermediaries between consumers and businesses, with the aim of preventing practices that may limit competition or create barriers to entry.

The first proceeding focuses on the operating system for mobile devices. The Commission intends to clarify how Google should grant third-party AI service providers free and effective access to essential functions of the system, including artificial intelligence based functions, such as the content-generation systems used by the platform itself. The aim is to ensure that third-party providers have an equal opportunity to innovate and compete.

The second proceeding concerns the search service. The act requires that competitors receive fair and non-discriminatory access to certain anonymized query, click and view data. The Commission will assess which information should be included, how it should be anonymized, and whether providers of conversational assistants or generative artificial intelligence systems can use this data to develop viable alternatives.

After analyzing these aspects over the coming months, the Commission will send its preliminary findings to Google and invite third parties to submit comments. The opening of these proceedings does not imply that an infringement has occurred, although nor does it prevent the Commission from imposing measures or sanctions in the future if a breach is ultimately found.

European Data Protection Board and European Data Protection Supervisor issue joint opinion on the proposal for a European Biotech Act

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have adopted a joint opinion on the European Commission's proposal for a European Biotech Act, aimed at strengthening the biotechnology and bio-manufacturing sectors in the field of healthcare. Both institutions support the creation of a single legal basis for the processing of personal data by sponsors and researchers, but caution that the high sensitivity of health and genetic data requires enhanced safeguards.

In particular, the opinion warns that the simplifications envisaged in the proposal — such as the harmonization of legal bases, the possibility of processing data for additional purposes, or the integration of new tools such as regulatory sandboxes or the use of artificial intelligence within the trial framework— must not lower the standards of protection under the GDPR. The EDPB and the SEPD recommend clarifying the obligations of data controllers, limiting retention periods, increasing the use of pseudonymization and ensuring that authorities only have access where strictly necessary. They also call for a more precise definition of the purposes of processing and the incorporation of additional safeguards where data is reused for other research projects.

European Union and Brazil adopt mutual adequacy decisions allowing personal data to flow freely

The European Commission has approved an adequacy decision recognizing that Brazil offers a level of data protection equivalent to that of the EU. At the same time, Brazil has adopted a reciprocal decision. This mutual recognition allows companies, governments, and research entities to exchange personal data between the two jurisdictions without the need for additional safeguards. The aim is to facilitate a secure flow of information and strengthen trust in economic and digital relations between the two regions.

Together they create the largest area of free and safe data flows in the world, benefiting a combined 670 million consumers, approximately, across the EU and Brazil. These decisions were adopted against the backdrop of the Partnership Agreement between the European Union and Mercosur and the recent Interim Trade Agreement, which seeks to strengthen economic and political ties between the two regions. The European decision follows an opinion by the European Data Protection Board and the EU member states' greenlight in the so-called comitology procedure.

The Commission will assess the functioning of its adequacy decision after a period of four years, after reviewing whether the necessary data protection safeguards remain in place.

European Commission designates WhatsApp as a very large online platform under the Digital Services Act

The European Commission has formally designated WhatsApp as a very large online platform under the Digital Services Act (DSA). This decision was prompted by the fact of its "Channels" feature exceeding the 45 million user threshold in the European Union.

Whereas the part of the app used for private messaging — chats between users, voice notes, photos, voice and video calls — falls outside the scope of the Digital Services Act, the Channels feature, on which recipients can disseminate information and updates to a broad audience, is classed as an online platform and is therefore subject to the obligations under the Act.

Following its designation, Whatsapp owner Meta has until mid-May 2026 to adapt and comply with the additional obligations applicable to very large platforms. These obligations include assessing and mitigating systemic risks, such as potential threats to freedom of expression, attempts at election manipulation, dissemination of illegal content, or privacy issues arising from the use of the platform.

Following this designation, the European Commission will be directly responsible for overseeing WhatsApp's compliance with the Digital Services Act, in collaboration with the Irish digital services coordinator.

South Korea launches the world's first comprehensive AI regulations

In January, the world's first comprehensive set of laws on artificial intelligence came into effect in South Korea, aimed at strengthening trust and security in the sector.

With a view to becoming one of the three AI powers worldwide, South Korea hopes that its new Basic AI Law will help place the country in a leading position in this field. The entire set of laws has come into force before the EU's AI Act, which will be implemented in phases until 2027.

Although the Basic AI Law has already entered into force and been implemented, however, the South Korean government has granted a one-year grace period to ensure or facilitate compliance with this law by companies and the various public agencies required to implement it. In this initial one-year phase, no investigations will be conducted and no fines will be imposed, although, after the end of the grace period, fines can be imposed up to 30 million South Korean won.

Decisions

AEPD fines an energy company due to shortcomings in its customer identity verification protocol

The AEPD has imposed a €1 million fine on an energy company due to a breach of article 32 of the GDPR, in relation to the security of personal data processing, after finding that the company lacked adequate security measures in its telephone-based customer identity verification system.

The penalty proceeding commenced following a complaint filed by a customer, who reported that his daughter's email address had been linked to his supply contract with another company in the same group, without either of them having provided that information or authorized such a change. Despite the respondent's argument that the change had been made in accordance with its identity verification protocol, the AEPD's investigation identified significant shortcomings in that system.

The AEPD identified several problems in the company's security protocol. First, the system allowed the customer's identity to be verified using information that could easily be known by third parties, such as the individual's full name, taxpayer identification number (NIF), or post code. Second, there was no record ensuring the traceability of the data provided during the telephone verifications, which made it impossible to accurately verify what information had been requested during each call. Third, the selection of which data should be verified was left to the discretion of each operator, with no standardized protocol to ensure a consistent level of security.

In addition to the financial penalty, the ruling ordered the respondent to adopt, within a maximum period of three months, appropriate technical and organizational security measures, including protocols that ensured the verification of the data subjects' identity before making changes to their contracts.

Healthcare facility fined for deleting a CD containing MRI scans provided by a patient

The patient who lodged the complaint with the AEPD had provided the hospital with MRI scans on CD which had been obtained previously, so that the facility could use them as a reference for a new diagnostic test. Months later, however, when the patient requested that they be returned, they were informed that the files had been deleted.

The AEPD concluded that these images constituted clinical documents for all intents and purposes, regardless of whether or not they had been included on the patient's medical records. Law 41/2002, of November 14, 2002, on patient independence and the rights and obligations concerning information and clinical documentation requires healthcare facilities to keep this type of documentation for at least five years. By destroying the scans, the hospital violated this duty of custody, which constituted unlawful processing without a legal basis.

In light of the above, the decision found that a threefold violation of the GDPR had taken place and imposed a fine totaling €1,200,000. First, it found that article 9 (special categories of data) had been infringed, because health data had been erased without meeting any of the exceptions that would have made their processing lawful, which resulted in a €100,000 fine. Second, it found that article 6 (lawfulness of processing) had been infringed, as the facility lacked a legal basis to justify the destruction of

the clinical documents, which resulted in another €100,000 fine. Lastly, article 25 (data protection by design and by default) was found to have been infringed, due to the absence of an adequate procedure for managing physical media containing health data provided by patients, an infringement subject to a €1,000,000 fine.

The AEPD underscored that this breach was not an isolated incident, and instead revealed a structural deficiency in the facility's procedures for the management, retention, and return of clinical documents provided by patients.

AEPD imposes €500,000 fine on a bank due to the loss of a customer's documentation

The decision was issued following a penalty proceeding filed against a bank due to the loss of the documentation provided by a customer in order to be added as a new authorized party on a bank account. The loss took place in the course of a courier service engaged by the respondent. The documentation that was lost included, among other items, a great deal of the complainant's personal data, including a full copy of their national identity card and that of their partner. The AEPD considered that it had been adequately proven that, following the collection of the documentation and despite the data subject's notices, the respondent had failed to activate effective traceability or early-warning mechanisms, limiting its response exclusively to partial and delayed enquiries, without identifying the processor until several months later.

Accordingly, the AEPD found that an infringement of article 32 of the GDPR had taken place, due to the failure to implement technical and organizational measures appropriate to the risk in order to ensure the availability, integrity, and confidentiality of the data – particularly with regard to the traceability of items sent and breach detection and management systems – within the framework of the accountability principle set out in articles 5.2 and 24 of the GDPR. The AEPD also referred to article 28 GDPR in relation to the selection and supervision of the processor, although it did not constitute a separate violation.

The respondent's negligence in relation to monitoring the incident was also highlighted and the AEPD took into account the sensitivity of some of the data affected (identity card and bank account details) and imposed a €500,000 fine. The proceedings concluded with a voluntary payment by the respondent, resulting in a reduction of the amount to €400,000, thereby rendering the decision final.

CNIL levies €42 million fine on a telecommunications group due to a security breach

The French data protection authority (CNIL) imposed two fines totaling €42 million on two entities in the same telecommunications group, following confirmation that a security breach had taken place that enabled a hacker to access information relating to more than 24 million subscriber contracts. The compromised data included bank identifiers, which are particularly sensitive due to their personal nature and the risks associated with their fraudulent use.

The authority's analysis revealed that several breaches of the GDPR had taken place. First, a breach of article 32 of the GDPR was established, because basic security measures that would have hindered the unauthorized access had not been implemented. Authentication to access the internal systems, including remote access by employees via VPN, was not sufficiently robust, and mechanisms to detect anomalous behavior had proven ineffective.

Second, a failure to comply with article 34 of the GDPR was identified in relation to the communication sent to the persons affected by the breach. The initial notification did not include all the information necessary to understand the scope of the incident, or the recommended self-protection measures, which hindered users' ability to respond promptly.

Lastly, in the case of one of the entities, responsible for mobile phone services, a violation of article 5.1.e) of the GDPR was also found to have taken place, due to the retention of data relating to former subscribers over several years, beyond the time necessary to fulfil the relevant accounting obligations.

Penalty imposed on energy supplier for cross-referencing the personal data of two customers

The breach occurred when a customer of the energy supplier received an email containing a third party's personal data, including their full name, contract number, bills, and information regarding the existence of a debt. The complainant had received this email because an employee of the energy supplier's data processor had mistakenly assigned the complainant's email address to the third-party customer.

The error occurred because the employee was simultaneously assisting two users via the chat channel, which led him to mistakenly enter the complainant's email address on another customer's file. This channel, which had recorded over 15,000 interactions in 2023, enabled an agent to manage multiple conversations at the same time, significantly increasing the risk of errors. Although the respondent deleted the channel in 2024, the AEPD considered this action to have been reactive rather than preventive.

Although the initial proposal was for a €1,000,000 fine, the decision ultimately imposed a €500,000 fine for the infringement of article 25 of the GDPR concerning data protection by design and by default.

The Agency concluded that the company lacked adequate technical and organizational measures to prevent inaccuracies in the data, such as effective controls to detect duplication or data being assigned to the wrong customers. The mechanisms in place only verified formal aspects but did not prevent the same data from being assigned to two different people. In the AEPD's view, the absence of adequate controls and risk assessments reflected a structural weakness in the data updating process, potentially exposing the company's entire customer base to similar incidents.

AEPD imposes fine on mobile phone company due to identity theft for a telephone line subscriber

The decision addressed a complaint lodged against a mobile telephone company due to the loss of the telephone service and the fraudulent banking transactions suffered by the complainant following an unauthorized change of ownership of the line and the creation of a duplicate SIM card.

In this case, a change of line ownership was processed over the phone without following the company's internal protocol, that is, without carrying out enhanced verification through a verification call to the line or sending an OTP (one-time password) and the verification of the final digits of the customer's bill. The call was not made from the line concerned. In relation to the duplicate SIM card, verification through a temporary code or phone call was not performed either and the scanned ID was that of a third party other than the complainant.

Accordingly, the AEPD held that neither the identification of the legitimate line holder, nor the lawfulness of the processing had been ensured, resulting in processing without a valid legal basis in breach of article 6.1 of the GDPR. Liability was based on a failure to exercise diligence in verifying identity, the breach of the accountability principle (articles 5.2 and 24 of the GDPR), and supreme court case law on identity fraud, which links liability to the absence of adequate controls to ensure a valid legal basis for processing.

Lastly, the AEPD considered that the existence of a single action had taken place, as two related unlawful processing operations had occurred – i.e. the change of line ownership and the issue of a duplicate SIM card. As a result, the Agency classified the action as a single infringement of article 6.1 of the GDPR and imposed a €300,000 fine.

AEPD reiterates that employees' personal cell phones cannot be used as an authentication tool in the workplace

The AEPD has once again ruled that the disclosure of employees' personal phone numbers by a contact center to one of its international clients, in order to activate a two-factor authentication system required to access corporate tools, is unlawful. This practice affected more than 200 employees and continued for over a year.

The company had implemented a system for accessing the tools of an international client which required employees to receive authentication credentials on their personal mobile phones. During initial training, employees were asked to write down their personal phone number and date of birth on a piece of paper Subsequently, they began receiving access codes directly from the client. Labor union representatives proposed alternatives such as using a corporate email, but the company replied that this was not feasible because the client required a phone number to be linked to generate a two-factor authentication token and the company did not have enough corporate devices. The company itself acknowledged that it was in the process of gradually transitioning to corporate phones and SIM cards, noting that 203 of the 364 employees were still using their personal phone numbers.

The Agency examined the case in light of article 6.1.b) of the GDPR, which only allows the processing of personal data when it is strictly necessary for the performance of the contract with the employee. In the AEPD's view, this requirement was not met, since it is the employer who must provide the material resources necessary to perform the activities in question, in line with the principle that the means of production belong to the employer in an employment relationship. For these reasons and given the existence of less intrusive alternatives (such as corporate email accounts or professional devices), the use of employees' personal phones could not be regarded as indispensable to provide the service.

The decision also underscored that the company was fully aware of the infringement: its data protection officer had warned in writing that the use of personal cell phones for professional purposes was in breach of the legislation. Despite this, the organization continued to send data to the client without providing technical alternatives or adopting adequate mitigation measures.

For these reasons, the authority held that an infringement of article 6 of the GDPR had taken place and imposed an €80,000 fine, which was ultimately reduced to €48,000 due to acknowledgment of liability and voluntary payment. It must be said that the ruling is somewhat inconsistent in its analysis of the company's role, initially classifying it as a data processor and subsequently as a data controller.

Potential changes to AEPD's criteria regarding the use of biometric technologies

The AEPD has set aside a case in relation to the use of biometric data to implement access controls to certain production areas by a company in the food sector.

This decision is of particular interest, because the AEPD finally closed the case without finding any infringement arising from the use of biometric identification technologies. The outcome may signal a potential shift in the AEPD's approach, which had previously been restrictive with respect to the use of such technologies for access control in the workplace.

In this case, according to the decision, the company justified the need for the control based on health requirements. It assessed alternatives, and restricted its deployment in the production area, rather than implementing it in a general and indiscriminate manner. Biometric control applied only to an area with restricted access for health reasons related to the food sector, which could justify the need for the measure.

Although the AEPD did not include in its decision a detailed analysis of the applicable legal bases or the potential legal basis for the processing of such data in accordance with article 9.2 of the GDPR, the ruling is nonetheless indicative of a possible shift in approach regarding the use of these technologies. Moreover, it outlines key guidelines concerning the requirements that must be met in order to implement these types of technologies in the workplace.

Penalty for the loss of medical records in a public place

The AEPD has imposed a €100,000 penalty on a company providing occupational health and safety services following an accidental exposure of medical examination records belonging to officers from various police forces. The documentation, which included particularly sensitive health-related data, was found

abandoned in the street after being transported from police premises to the company's facilities.

The investigation revealed substantial flaws in internal procedures: the absence of a chain of custody, the lack of records regarding the transfer of the documentation, and the absence of organizational measures to ensure its confidentiality. The authority concluded that these facts constituted a violation of the principle of integrity and confidentiality under article 5.1.f of the GDPR, which justified the fine.

Apart from the fine, the decision also ordered the company to implement measures ensuring the traceability and protection of medical documentation when it is handled outside its facilities. The AEPD noted that the processing of health data requires extra diligence and that those responsible for these types of services must ensure that security measures proportionate to the risk arising from their activities are in place.

Hotel fined for unlawful disclosure of customers' personal data

In this decision, the AEPD examined a complaint submitted via the IMI System (Internal Market Information System) by the Swedish Data Protection Authority against a hotel company, in connection with an unlawful disclosure of personal data relating to property owners and guests staying at a holiday resort.

The security staff, acting as data processors engaged by the company, left lists in writing in plain sight which contained data such as first and last names, country, apartment number, passport details and national identity card numbers, making them accessible to third parties, who even went so far as to photograph them. The AEPD verified that although the company had generic protocols in place and had subsequently provided documentation on audits, internal protocols, and measures adopted, it had not been established that adequate technical and organizational measures had been implemented to prevent unauthorized access to the data. The AEPD therefore concluded that a breach of confidentiality had taken place and that the measures relied on were inadequate and insufficiently defined to meet the GDPR's security requirements.

A €40,000 fine was imposed, taking into account the nature and seriousness of the infringement, the volume of data exposed, the sensitivity of the information involved (national identity card and passport details), and the fact that the controller's activities entailed the ongoing processing of personal data. The company opted for voluntary payment, leading to a 20% reduction in the fine, which was therefore set at €32,000. The decision also required the company to evidence, within three months, that it had implemented appropriate measures to prevent similar incidents.

Dental practice fined for recording video and audio inside the clinic

The decision examined a case in which a former employee of a dental practice reported the recording of images and sound through video surveillance cameras without proving adequate information, alleging that no visible notices were displayed and that patients were not informed of the recording during clinical procedures. The respondent stated that there were two devices: a video camera located inside the dental treatment room and a photographic camera in the reception area, both intended for security purposes and managed by an external provider. It acknowledged that the system recorded audio within the treatment room and that the images were kept for a maximum period of seven days.

The AEPD considered that the continuous recording of patients during dental treatments was disproportionate to the security purposes invoked, which breached the data minimization principle under article 5.1 c) of the GDPR. The Agency underscored that the recording of conversations between patients and employees constitutes an unlawful encroachment on the right to privacy and ordered that the camera be refocused or removed within three months.

The decision imposed a €2,000 fine, because the infringement comes under article 83.5 of the GDPR (basic principles and conditions of lawfulness), taking into account the nature of the facts, their scope, and the impact on fundamental rights. During the course of the proceedings, the dental practice accepted responsibility and elected for voluntary

payment, which resulted in the fine being reduced to €1,200. The AEPD found that an infringement had taken place, upheld the applicable fine, and drew the proceedings to a close.

Healthcare union and its foundation fined for a data breach and lack of transparency regarding their shared responsibility

The supervisory authority has fined a labor union in the healthcare sector, and its foundation – linked to nursing training, €15,000, after identifying two serious infringements in connection with a ransomware attack that compromised the personal data of almost 198,000 individuals. Both entities acted as joint controllers in the conduct of their joint training program for healthcare professionals.

The incident occurred when a group identified as Hunters International gained access to their systems, encrypted the data, and publicly announced the alleged sale of databases on the dark web. Although the notification submitted to the authority stated that only the data managed for training purposes had been affected, the investigation revealed that other areas might also have been compromised. The authority indicated that there was no record of notifications having been sent to potential data subjects not involved in the training, raising doubts as to whether the real scope of the breach had been properly defined.

The decision concluded that article 5.1.f) of the GDPR had been breached, on the grounds that neither a sufficient risk assessment nor appropriate technical and organizational measures had been implemented prior to the attack. The shortcomings identified included: the absence of multi-factor authentication, unencrypted databases, insufficient capacity to detect and assess the incident properly, and a lack of oversight regarding its impact and duration.

In addition, the authority considered that article 26 of the GDPR had been infringed, after finding that the two entities had declared themselves joint controllers on the basis of a generic agreement and had failed to transparently set out their respective responsibilities. Nor was that agreement made available to the individuals participating in the training activities and the information provided in forms and privacy policies did not reflect the actual joint responsibility shared by the two organizations.

AEPD fines telecoms operator for sending customer login credentials in a plain-text email

The AEPD has issued a decision imposing a €10,000 fine on a telecommunications operator for an infringement of article 32 of the GDPR. The proceeding commenced following a complaint from a customer who had received an email, sent in plain text and without encryption, that both notified the customer of an update to their customer services while also explicitly including their full login credentials (username and password). The complainant reported that the portal, which stores data such as first and last names, address, ID number, phone number, bank account, invoices, and usage details, also lacked two-factor authentication.

The company argued that the incident stemmed from an isolated human error, that it took immediate action by resetting the passwords and contacting the affected customer and that no unauthorized access or data exfiltration had occurred. However, the AEPD rejected these arguments, pointing out that article 32 of the GDPR establishes an obligation of means that requires security measures to be effectively in line with the risk and that sending credentials in plain text by email demonstrates the absence of sufficient organizational measures to prevent an unlawful disclosure of authentication information. The Agency further stressed that an infringement does not require that actual damage occurred; it is sufficient for the security measures to be inadequate in relation to the inherent risks of the processing.

As mitigating factors, the AEPD took into account the company's swift response and the corrective measures it had adopted. As aggravating factors, it cited gross negligence in relation to compliance and the fact that the company's activities involved the large-scale processing of customers' personal data.

AEPD fines online lending company for requiring customers to submit a photo with their ID to process a loan cancellation

The AEPD has issued a decision fining an online lending company for breaching article 5.1.c) of the GDPR, in relation to the principle of data minimization. The proceedings commenced following a complaint from a customer who, after requesting early repayment of their loan, received a request – as a condition for processing the request – to submit a photograph showing them holding their identity document.

The company argued that this identification procedure was required to comply with its obligations under anti-money laundering rules. The AEPD rejected this argument, noting that the sector-specific legislation relied upon was neither contrary to nor incompatible with the principles of the GDPR, and that both sets of rules had to be applied concurrently. In particular, the Agency underscored that Anti-Money Laundering Law 10/2010 of April 28, 2010 establishes an identification obligation that can be fulfilled by other, less intrusive means, such as qualified electronic signatures, copies of identity documents issued by a public notary, or verification through identification systems already enabled by the company for its customers. Requesting a photograph of the data subject holding their ID document constitutes an excessive processing of personal data and creates additional risks of identity theft.

The fine that had initially been proposed was €10,000, although the company opted for voluntary payment with a 20% reduction, which set the fine at €8,000. In addition, the AEPD ordered the company to implement measures to ensure that identity verification in loan cancellation procedures is carried out in the future using methods that comply with the principle of data minimization.

AEPD upholds a complaint against the Balearic Islands Health Service over failure to comply with a citizen's right of access

The AEPD has rendered a decision on the proceeding concerning data subject rights, which commenced following a complaint by a citizen who exercised their right of access against the Balearic Islands Health Service (IBSALUT), after the request failed to receive the response required by law.

The AEPD's decision noted that, under article 12 of the GDPR and the Law on Data Protection and the Safeguard of Digital Rights (LOPD-gdd), the data controller must put in place appropriate procedures and mechanisms to facilitate the exercise of rights by data subjects, and is required to respond to requests within one month, stating its reasons where it intends not to comply with the request. The burden of proof regarding compliance with the duty to respond to the data subject's request to exercise their rights lies with the controller and any communication addressed to the data subject must be concise, transparent, intelligible, and easily accessible and use plain and clear language.

The AEPD further stated that the applicable rules do not allow requests to be disregarded as if they had not been submitted. Data controllers are required to issue a reply in all cases, even where no personal data relating to the individual are being processed or where the request does not meet legal requirements. In such cases, the recipient is also required to request that any identified deficiencies be remedied or, where appropriate, to refuse the request with proper justification, stating the reasons why the exercise of the right in question cannot be upheld.

Consequently, the AEPD upheld the complaint, finding that article 15 of the GDPR had been infringed, and urged the Balearic Islands Health Service within ten business days from the date on which the decision became final and enforceable, to provide the complainant with a certificate either granting the right of access exercised, or to issue a reasoned refusal, stating the grounds for not granting the request.

AEPD fines a courier company for unauthorized subprocessing in the processing chain

The AEPD has fined a company in the logistics sector for various irregularities in the management of sub-processing within the processing chain. The case arose when a customer discovered that in order to manage a delivery, their personal data had been disclosed to third parties who were not included on the list of authorized processors.

After analyzing the documentation provided by the companies involved, the AEPD concluded that three distinct violations of the GDPR had occurred. First, the company acting as processor engaged an unauthorized subprocessor (a company specialized in logistics), thereby infringing article 28.2 of the GDPR, which requires the controller's prior and specific consent. Second, it failed to adequately inform the controller that this subprocessor had in turn engaged a third party, thereby reinforcing the violation of the same provision. Lastly, the AEPD noted that no valid sub-processing agreement had been signed between the defendant and the first subprocessor, in violation of article 28.4, which requires that the obligations applicable to the processing be documented.

Each of these violations is punishable by a separate €5,000 fine , bringing the total amount to €15,000.

Healthcare provider mistakenly sends personal data of assisted reproduction patients to other service users

In April 2023, the AEPD received a complaint in which an individual reported that the assisted reproduction unit at the facility where they had been a patient had sent them an email announcing the transfer of the service to a new entity, which included the personal data of other patients.

The respondent used an automated system based on merged Word and Excel documents containing patients' personal data (first name, surname, national ID number and email), generating PDF files that were automatically sent by email. The process worked correctly for the first 299 emails, but from the 300th document onwards it began sending information to the wrong recipients. Consequently, at least 237 patients received personal data belonging to other users (first name, last name, ID number, and their status as assisted reproduction patients), out of a total of 637 individuals who had potentially been affected. The breach was reported to the AEPD and the data subjects.

The AEPD identified two breaches of the GDPR in this penalty proceeding: (i) a breach of the principle of integrity and confidentiality (art. 5.1.f) for failing to encrypt the notifications despite internal requirements, and (ii) non-compliance with article 35 for failing to conduct a data protection impact assessment (DPIA) for the large-scale processing of health data. The AEPD dismissed the respondent's arguments that the processing predated the GDPR and had been adapted through a risk analysis, and underscored that a 2020 audit had already identified the need to conduct a data protection impact assessment (DPIA).

The AEPD proposed a fine totaling €100,000 (€50,000 per infringement). Following voluntary payment with a 20% reduction, the fine was finally set at €80,000.

Fine imposed for unlawful processing of biometric data and excessive retention of personal data

The AEPD has imposed a €950,000 fine on a company specializing in identity and age verification in digital environments, for processing biometric data without a legal basis under article 9.2 of the GDPR, obtaining invalid consent, and storing data for longer than necessary.

When registering for the service, users undergo a verification process during which their facial image is captured. That capture is then used to generate and store a biometric template, which is employed to authenticate the user and verify their identity in subsequent accesses or interactions. The AEPD concluded that this process involved uniquely identifying an individual, which constituted the processing of special categories of data in accordance with article 9.1 of the GDPR. The company argued that its system did not "identify" the user.

However, by failing to recognize the special nature of the data processed, it had not applied any of the legal bases under article 9.2 of the GDPR, and therefore the consent obtained was deemed invalid.

The decision also penalized the practice of obtaining consent for research and service improvement purposes through pre-ticked boxes, which is incompatible with the GDPR requirement that consent be free, specific, informed and unequivocal (article 7). Finally, a breach of the storage limitation principle was found, as personal data had been stored for a period longer than strictly necessary, without effective criteria for erasure (article 5.1 e) of the GDPR).

AEPD fines company for unlawful processing of personal data by one of its sales representatives

The AEPD has issued a decision imposing a €20,000 fine and a further €200,000 fine on an energy sector company due to a breach of articles 13 and 6 of the GDPR, respectively.

The dispute arose following a telephone call made to an individual by a sales representative of the respondent company, which was subsequently followed by an email sent to the same individual in which their personal data had already been included. As in numerous other similar cases, the complainant argued that they had had no prior contact or relationship with the defendant, whose products and services were being promoted by the sales representative.

The respondent argued that at the time the communications were sent, the sales representative was acting as an independent data controller and that, therefore, any unlawful processing of personal data on their part should, where applicable, give rise to liability on the part of the sales representative rather than the respondent company. However, the AEPD carried out a detailed analysis of the definitions of controller and processor, concluding that, in light of the circumstances of the case, the respondent determined the purposes and means of the processing and was therefore, in fact, the data controller. As a result, the AEPD found that the respondent had breached both its duty to provide information and the requirement to have a valid legal basis for making those communications, given that it had no relationship whatsoever with the complainant.

The decision offers key insights when determining roles and serves as a warning against common practices in certain sectors, where individuals' information is shared all too freely among commercial companies and different service providers.

Fine resulting from a security incident

In this decision the AEPD found that articles 5.1.f), 32, 33 and 34 of the GDPR had been infringed following a security incident suffered by the respondent, which affected up to one million records, and imposed a fine totaling €1,090,000.

Although there are many similar decisions which, as in this case, focus on the level of diligence exercised by the entity in implementing security measures and managing the incident, this decision is particularly noteworthy in that it refers to issues which, while already well known, are nonetheless highly relevant and of interest. They notably include the following:

- The 72-hour period for notifying the AEPD of the security incident must be calculated in calendar days and the fact that the deadline falls on a public holiday is not a valid reason for delaying the notification.

- The AEPD imposed a joint penalty for the infringement of both articles, namely 5.1.f) and 32 of the GDPR, as it has done on numerous occasions. Although it is true that more recent decisions had limited findings of infringement to one of the two articles rather than both jointly, the AEPD has returned to this approach, arguing that such a "dual" sanction does not constitute a breach of the *non bis in idem* principle and that they are both fully compatible.

This issue is the subject of ongoing debate both in the AEPD's decisions and before the courts, making it important to monitor developments closely in order to remain up to date with its progress.

Judgments

CJEU rules on national legislation regarding the processing of biometric data

In this judgment the TJUE has ruled on various referrals for a preliminary ruling regarding the application of French national legislation transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

The case originated in France, where an individual was arrested during a demonstration and refused to be fingerprinted and photographed. Although he was acquitted of the main offense under investigation, he was ordered to pay a fine of 300 euros for refusing to provide identifying information, pursuant to article 55-1 of the French Code of Criminal Procedure. Following simultaneous appeals, the French courts referred three questions to the CJEU for a preliminary ruling to determine the compatibility of that legislation with the aforementioned Directive (EU) 2016/680.

The debate focused primarily on the extent to which national legislation might require the collection of particularly sensitive data, such as biometric data. In this regard the CJEU concluded as follows:

- National legislation providing for the systematic collection of biometric data from any person suspected of having committed or attempted to commit a criminal offense is contrary to EU law, unless two conditions are met: (i) national law must define in an appropriate and sufficiently precise manner the specific purposes of the collection of such data, and second, (ii) the competent authority is required, in each individual case, to assess whether the collection of that data is strictly necessary to achieve those purposes, so that the collection of that data is not systematic.

- The competent authority must provide adequate justification, in each specific case, as to why the collection of biometric data is "strictly necessary." The court clarified that such justification may be succinct, provided that it is sufficiently clear in order to allow the data subject to understand the reasons for the measure and to be able to exercise their right to an effective remedy.

- Regarding the lawfulness of the penalty for failing to cooperate with the authorities, the CJEU concluded that EU law does not preclude a member state from imposing criminal penalties for refusing to consent to the collection of biometric data. However, this penalty is only lawful if the data collection meets the requirement of being "strictly necessary" and if the penalty imposed respects the principle of proportionality.

This judgment is of particular interest in the context of the activities of law enforcement agencies, as it provides important guidelines on their powers and the requirements that must be met in the national legislation to authorize the collection of certain types of data by these agencies.

WhatsApp Ireland's appeal against the binding decision of the European Data Protection Board is admissible

The case addressed in this decision dates back to the proceedings initiated in December 2018 by the Irish Data Protection Authority (Data Protection Commission or DPC), as the lead supervisory authority, against WhatsApp Ireland Ltd (WhatsApp) due to the purported breach of the transparency and information obligations set forth in articles 12 to 14 of the GDPR. In this regard, following an initial draft decision issued by the DPC and submitted to the other national supervisory authorities concerned, eight of them raised relevant and reasoned objections, which led to the referral of the dispute to the European Data Protection Board (EDPB) pursuant to article 65(1)(a) of the GDPR.

In this regard, in July 2021, the EDPB issued Binding Decision 1/2021, which found that there had been a violation of the aforementioned provisions of the GDPR, and required the DPC to amend the proposed corrective measures and, in particular, the amount of the fines. Based on the foregoing, the DPC issued a final decision in which, among other measures, it imposed a series of fines on WhatsApp totaling €225 million.

In response to this ruling, WhatsApp brought an action for annulment against the EDPB's binding decision before the General Court. However, the General Court declared the action inadmissible because the decision did not did not constitute an 'act open to challenge' and did not directly affect WhatsApp. In this regard, the General Court held that the decision was an intermediate measure (not final) and that only the final decision could be challenged before a national court. In response to this ruling, WhatsApp filed an appeal before the CJEU, which was resolved in this judgment.

The judgment addresses two main legal issues: (i) whether the EDPB's binding decision was open to challenge and (ii) whether the measure was of direct concern to the applicant.

First, regarding the nature of an act that may be challenged under article 263 of the Treaty on the Functioning of the European Union (TFEU), the CJEU notes that an action for annulment may be brought against any act adopted by the institutions, bodies, offices and agencies of the Union intended to produce binding legal effects. In doing so, it is necessary to consider the substance of the act in the light of objective criteria such as its content, the context in which it was adopted and the powers of the body that adopted it, among others. In this regard, the CJEU expressly rejects the General Court's classification of the act as an "intermediate measure", clarifying that the EDPB's decision definitively establishes that body's position on the issues it must resolve, thereby exhausting its scope of competence.

Regarding the requirement of direct concern set forth in article 263 CJEU, paragraph 4, the Court applies its established case law, which requires the fulfillment of two cumulative conditions: the act must directly affect the applicant's legal situation and must leave no margin of discretion to the addressees who are entrusted with the task of implementing it. Consequently, the CJEU concluded that the EDPB's decision brought about a distinct change in WhatsApp's legal situation. It held that additional infringements of the GDPR had taken place – specifically articles 13.1.d) and 13.2.e) – which compelled the company to change its contractual relationship with the users of the messaging service provided by WhatsApp, from which it followed that there was a direct link between that decision and its effects on WhatsApp's situation.

Based on the above, the CJEU declared the action for annulment brought by WhatsApp admissible, set aside the order of the General Court and referred the case back to it for a ruling on the merits, including the question of whether WhatsApp had breached the transparency and information obligations set forth in articles 12 to 14 of the GDPR.

Annulment of several fines imposed by the AEPD on an insurance company for sending commercial communications to generic email addresses

Panel One of the Judicial Review Chamber of the Supreme Court upheld the appeal filed by a well-known insurance company against the decision issued by the AEPD in April 2022, confirming three fines it had imposed, of €100,000 each, for each one of the

infringements of articles 6, 28 and 17 of the GDPR.

The penalty proceeding had originated from a complaint filed by an individual who, between 2016 and 2020, repeatedly requested the deletion of their personal data without receiving a response, while continuing to receive advertising communications at a generic email address (info@…), which was registered on the Robinson List.

The chamber based its decision to uphold the appeal on several grounds. First, it found that a generic email address such as info@company.com did not qualify as personal data within the meaning of article 4 of the GDPR, as this does not enable a specific individual to be identified either directly or indirectly. Second, it determined that the data controller was not the insurance company *per se*, but rather the insurance agents who, acting independently, collected and managed the data as independent controllers, without any evidence of a shared database. Finally, the Court noted that, once the complainant's objection was brought to the insurer's attention, they were informed that no personal data were held in its systems and were removed from the agents' distribution lists.

Consequently, the National Appellate Court set aside the three fines imposed and expressly ordered the defendant authorities to bear the costs.

National High Court upholds the dismissal of a complaint concerning the loss of a medical report, finding the events to be time-barred

Following the filing of a complaint with the AEPD regarding the loss of a 2015 medical report concerning the claimant's father – which, according to the claimant, was proof of a security breach – the AEPD dismissed the complaint on two grounds: the statute of limitations on the claims and the inapplicability of data protection regulations to deceased persons, except as provided for in article 3 of the LOPD-gdd.

On appeal, the National Appellate Court upheld the AEPD's dismissal, although it qualified certain aspects of that decision. First, it agreed that the facts were indeed time-barred. However, it rejected the argument relating to the legal regime applicable to deceased persons, since at the time the lost report was prepared, the patient was still alive. Second, the Court clarified that the incident did not constitute a system security breach, but rather a matter of document management and record-keeping, as the physician had regarded the document as a draft and therefore did not include it in the medical record.

The judgment also addressed the claimant's standing, acknowledging that they did have a legitimate interest in requesting an investigation into the facts related to data processing. However, it noted that this right did not entail the power to initiate disciplinary proceedings or to impose specific fines.

As a result, the National Appellate Court dismissed the appeal and upheld the AEPD's decision, without imposing costs.

Fine overturned on member of labor union staff committee for forwarding corporate emails to recipients outside the committee

The National Appellate Court has rendered a decision on an application for judicial review filed against an AEPD decision dated August 30, 2022, issuing a €2,000 fine for an infringement of article 6(1) GDPR, as defined in article 83(5) GDPR and article 72(1)(b) of the Spanish Data Protection Law.

The AEPD found that a member of a union's staff committee had repeatedly forwarded emails containing data on another committee member (the complainant), such as the complainant's name and work email address, to other individuals, both members and non-members of the staff committee, as well as to corporate email addresses of unions and organizations, without authorization to do so, without the data subject's consent and despite the data subject's express objection on several occasions.

In its decision, the AEPD found that this qualified as unlawful processing of personal data, taking into consideration that the processing of the complainant's personal data had been excessive, because the emails

mentioned in the complaint were also sent to individuals outside the staff committee.

An application for judicial review against this decision was filed with the National Appellate Court, in which the applicant alleged that the use of email fell within the scope of labor law and was part of his union duties, together with the fact that all the recipients were civil servants or union representatives and they all had access to the data at issue in the complaint on the Employee Portal, such as the corporate email address the complainant's name and professional category, the destination and the complainants phone number.

The National Appellate Court recognized that a corporate email address is an item of personal data if it contains the name of a specific user, in line with the Agency's own determinations in Report 0437/2010. It concluded, however, that it cannot be ignored that dissemination of the email address took place exclusively within the scope of the civil service and in a specific area of the organization, and the recipients were public officials or labor union organizations which strictly speaking cannot be considered third parties unrelated to the information that the staff committee sent.

The chamber highlighted further that all the recipients had been given authorization to access the Employee Portal, so the disseminated data had already been published, or consent had been given in relation to their dissemination, at least in that context, because they qualify as data made public under 9.2.e) GDPR. For all these reasons, the appellate court held that the processing cannot be classified as unlawful, upheld the appeal and overturned the AEPD's decision.

A debt collection company does not violate the right to honor if it evidences a prior request for payment before including data on a delinquency file

In this judgment, the Supreme Court examines whether the inclusion of a debtor's data on a credit risk file qualifies as an unlawful infringement of their right to honor where there is evidence that a prior request for payment was sent but there is no verifiable proof of its receipt.

The dispute stems from a lawsuit filed by an individual against a company engaged in managing and acquiring past-due debts, which had reported his data to the Asnef-Equifax database in relation to a debt under a phone contract. The claimant submitted that the inclusion of his data was unlawful because no evidence had been provided of effective receipt of the prior request for payment and requested cancellation of the data plus moral damages. Both the court of first instance and the provincial appellate court upheld the claim due to holding that insufficient proof had been provided of receipt of the request.

An appeal lodged by the respondent was upheld by the Supreme Court and the earlier judgments were overturned. The chamber recalled its settled case law to the effect that the requirement for a prior request does not entail an obligation to provide verifiable proof of its receipt, and reasonable evidence that it was sent correctly is sufficient. In this specific case, the request was sent by postal mail to the address provided by the debtor himself in the contract, there is no record that it was returned and no evidence was provided that would cast doubt as to whether it arrived at the recipient's address.

The court noted further that the debt was determinable, due and payable, and this was not disputed in the claim. It concluded therefore that there was no unlawful encroachment on the right to honor and ruled to dismiss the claim in its entirety with an award of costs against the claimant in the case at first instance.

Supreme Court overturns violation of right to honor on the ground of inclusion in a credit risk file of data relating to a tax debt obtained from an official gazette

The Supreme Court has upheld an appeal lodged by a credit reporting company, and overturned the judgment by Madrid Provincial Appellate Court which had held that there had been an unlawful encroachment on the claimant's right to honor and ordered the company to pay €4,000 in moral damages.

The dispute arose from the inclusion of the claimant's data on a credit risk file, following

publication in the Official State Gazette of a notice of seizure in respect of a tax debt owed to Madrid City Council. The entry remained in effect between February 2017 and May 2021 and was seen by two banks, which led to the denial of a loan to the data subject.

The point of law qualifying for an appeal consisted of determining whether the requirements under subarticles 2 and 4 of article 29 of the repealed Organic Law 15/1999 (prior request for payment, notice of inclusion and subsequent notification) are applicable to the files under subarticle 1 of the same article, which are populated with data from publicly accessible sources. Reiterating the principles adopted in judgments 434/2023 and 917/2025, the Supreme Court concluded that those principles do not apply to these files, which are governed exclusively by the general provision in the law and its regulations.

The chamber therefore upheld the appeal, confirmed the first-instance judgment, which had dismissed the complaint due to considering that the data were accurate and obtained from a public source, and ordered the claimant to pay the costs of the appeal.

Supreme Court recalls key issues in relation to the inclusion of data in credit reporting systems

This judgment examines the lawfulness of the processing of personal data on credit reporting systems and its impact on the right to honor, in a decision on an appeal lodged by a company against a judgment holding that the claimant's right to honor had been violated due to incorrect inclusion on that file.

The court addressed three key issues regarding data protection:

- Data quality principle: only certain, overdue, and enforceable debts may be recorded on credit files. This inclusion was unlawful because the debt was not substantiated, as there were discrepancies between the amount transferred and the amount certified by the assigning entity.
- Prior request for payment: the court acknowledged the functional nature of the request but established that it loses relevance where the debtor is already listed in delinquency files due to prior entries by other entities.
- Compensation regime: a distinction is made between a violation of the GDPR (which requires proof of damage, under article 82.1 GDPR and CJEU Case C-300/21) and a violation of the right to honor, where the legal presumption of damage under art. 9.3 of Organic Law 1/1982 applies.

The decision partly upheld the appeal and reduced the compensation from €7,000 to €3,000.

Fine for unlawful processing of data related to a credit card debt overturned, although the court upheld the fine for violation of the right of access

The judgment partly upheld an application for judicial review filed by a debt management company against an AEPD decision that had issued two penalties for infringement of the GDPR in relation to a claim for a credit card debt. The National Appellate Court overturned the €30,000 fine for a purportedly unlawful processing of data (article 6.1 GDPR) and confirmed the fine for the same amount issued for failure to exercise diligence in dealing with the right of access (article 15 GDPR).

The case stemmed from a complaint by a consumer who received a request for payment of a credit card debt which she claimed she was unaware she had contracted. The National Appellate Court found sufficient evidence that the contract had been concluded by phone in October 2000 (despite the absence of a recording of the call or a signed contract), based on the presence of the data subject's personal data, use of the card until 2004, subsequent payments associated with the transaction number, and a notification of transfer of the debt in 2008, without any objection from the data subject. Based on this, the National Appellate Court concluded that the processing was based on performance of the contract (art. 6.1.b GDPR), that there was unequivocal consent from the data subject, and that therefore the processing must be considered lawful.

The National Appellate Court did, however, confirm the fine for infringement of article 15

GDPR, because the claimant only dealt with the request for access after the data subject filed a complaint with the AEPD, and had not provided evidence of adequate prior steps or compliance with the legally stipulated time limit. The judgment reiterated the obligation to deal with requests to exercise rights and to provide a reply within one month with clear, accessible, and traceable information, under article 12 and article 15 GDPR.

Confirmation of lawfulness of personal data processing for the ASNEF credit risk register

The Supreme Court has dismissed an appeal lodged by an individual against a judgment by Madrid Provincial Appellate Court, confirming the lawfulness of the inclusion of her personal data on the ASNEF file at the request of a microloan lender.

The case stemmed from a €200 microloan entered into electronically in December 2017. Following default by the borrower, the lender sent 22 emails claiming payment and a letter by post (returned with a note saying "not known") before entering the data with ASNEF in March 2018. The borrower did not file an objection either in the subsequent debt collection proceedings, which concluded with a debt enforcement order.

From a data protection standpoint, the court first examined the data quality principle and found that the debt was determinable, due, and payable, as evidenced by the contract documents and the debtor's conduct in the proceedings. Secondly, in relation to the prior request for payment, the court reiterated its principle on the functional nature of that request: it is a guarantee designed to prevent the inclusion of individuals who have failed to make payment due to a simple oversight or error, making this information irrelevant for assessing their creditworthiness. In this case, the chamber disregarded any element of surprise in view of the nature of the contract, the existence of prior entries on the ASNEF file for debts with two other institutions, and the debtor's failure to reply to the claims. As a result, any formal defects in documenting the request do not, in and of themselves, constitute unlawful processing. Lastly, it rejected that the minimization principle under article 5.1.c) GDPR disallows the inclusion of a party for small debts, since finding otherwise would mean a debtor who repeatedly defaults on small amounts of debt would not be captured by the system.

Worker's data protection right held to be violated after her name and pay details were disclosed in a dismissal letter sent to her partner

The Canary Islands High Court held that the fundamental right to data protection had been violated for a worker at a supermarket chain. The issue concerned a dismissal letter sent to the worker's partner, an employee at the same chain. To substantiate that she had received a pay supplement incorrectly, the employer included the employee's name and salary in the letter as a point of reference, because they both worked the same hours. The employer was ordered to pay her €7,500 in compensation.

The court recognized the employer's legitimate purpose in exercising disciplinary authority and in providing reasons for the dismissal, although it held that the disclosure of personal data without the data subject's consent was disproportionate. The employer could have achieved the same aim by making the comparison without mentioning anyone by name, which is a more moderate yet equally effective measure for achieving that purpose, and it would have been sufficient to mention another worker in the same position or to use anonymized data. The court's analysis was based on article 5.1 and article 6.1 GDPR, and it highlighted the proportionality requirement in the workplace.

Contact our professionals

Alejandro Padín
Partner - Madrid
alejandro.padin@garrigues.com

Luisa Cyrne
Principal associate · Lisbon
luisa.cyrne@garrigues.com

Álvaro Blanco
Senior associate · Madrid
alvaro.blanco@garrigues.com

Andrea Ugalde
Associate · Bilbao
andrea.ugalde@garrigues.com

Garazi Tomás
Associate · Bilbao
garazi.tomas@garrigues.com

Ignacio Suárez
Associate · Madrid
ignacio.suarez@garrigues.com

Laia Llambrich
Associate · Bilbao
laia.llambrich@garrigues.com

Franco Muschi:
Partner· Lima
franco.muschi@garrigues.com

Adrian Leon
Senior associate · Alicante
adrian.leon@garrigues.com

Mariana Ubidia
Senior associate · Lima
mariana.ubidia@garrigues.com

Carina Casadesús
Associate · Barcelona
carina.casadesus@garrigues.com

Iciar Velasco
Associate · Madrid
iciar.velasco@garrigues.com

Javier Enebral
Associate · Madrid
javier.enebral@garrigues.com

Marta Sabio
Associate · Barcelona
marta.sabio@garrigues.com

More information:
Data Economy, Privacy and Cybersecurity

GARRIGUES

Plaza de Colón, 2 - 28046 Madrid
T +34 91 514 52 00

info@garrigues.com
garrigues.com

Follow us on: