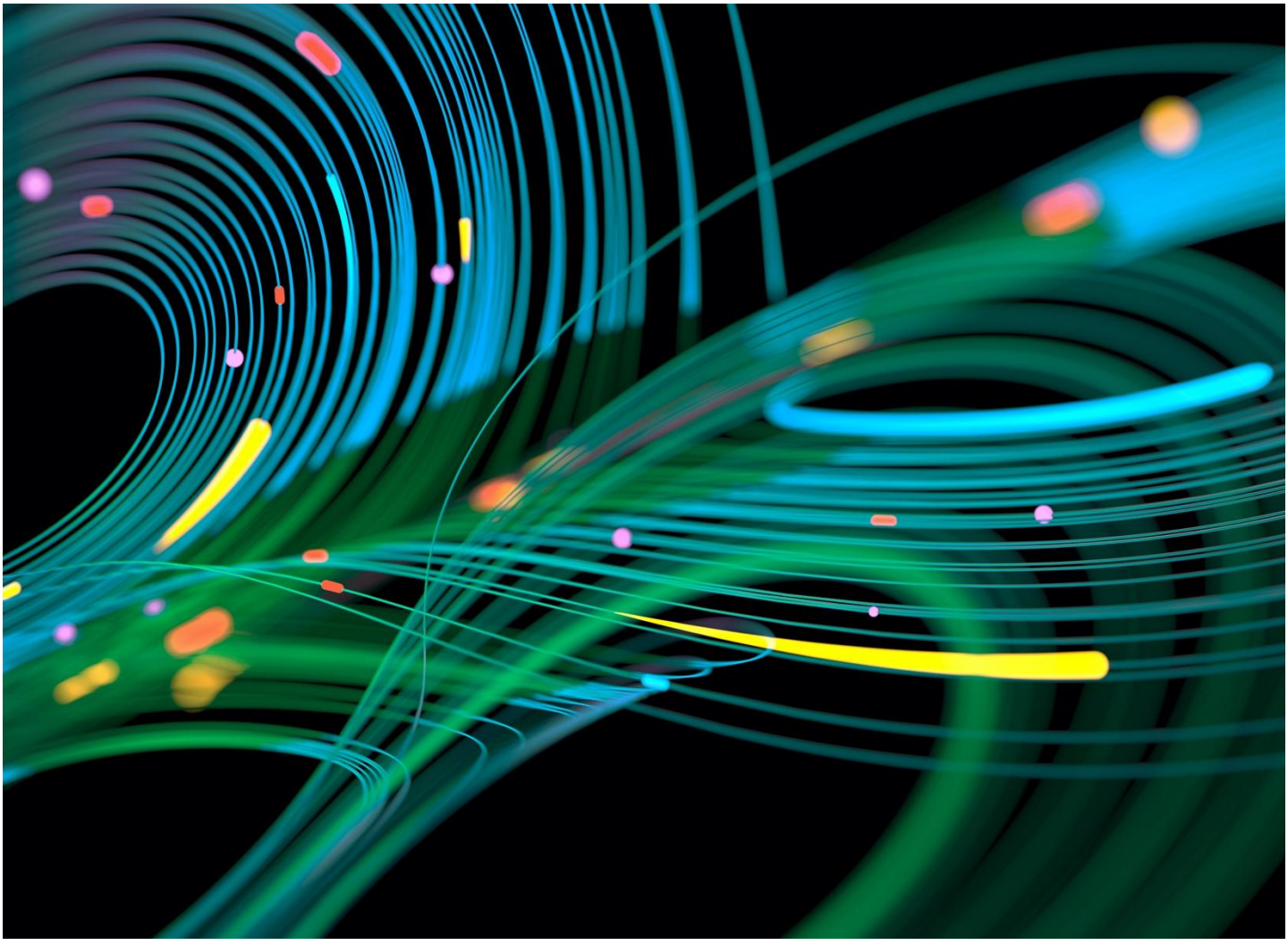
GARRIGUES

Data Economy, Privacy and Cybersecurity Newsletter

October 2026

The latest news in digital law and technological innovation, featuring recent rulings and key judgments on AI, e-commerce, and technology regulations



The digital duty of care: the personal liability of boards and their members in relation to technology risks



Alejandro Padín

Cybersecurity is no longer simply a technical issue. It has now become an essential corporate governance responsibility. The convergence of European laws on cybersecurity, digital resilience, and artificial intelligence is shaping a new duty of care for directors, requiring their direct and continuous involvement in managing technology risks and potentially giving rise to personal liability implications.

Until very recently, cybersecurity fell within the responsibilities of chief information officers or heads of IT security. Boards of directors only dealt with this subject, if at all, following a major incident and to manage its financial or reputational consequences. This was a technical matter, unrelated to corporate governance, that did not regularly feature on their agenda or create personal concern among directors. Today, that blithe delegation of responsibility has become a legal risk for every director.

The European Union has now produced an extensive collection of laws and regulations on the subject (NIS 2, DORA, the Cyber Resilience Regulation, the GDPR, and the Artificial Intelligence Act). This article does not aim to provide an exhaustive analysis of any of these laws regulations, but rather to present a proposition that is especially important for senior management: the convergence of these laws and regulations is, in fact, giving rise to a new standard of care or directors and senior executives concerning cybersecurity and technology risk. We refer to this below as the digital duty of care.

Legislative convergence: a mesh of obligations directed at managing bodies

In just a few years, European lawmakers have adopted legislation with a variety of purposes and scopes, although they all share a common feature: they impose direct, rather than simply delegable, obligations on the highest governing body of the organizations in their scope. This is no coincidence, it is a legislative policy decision. These are the main components of that mesh of laws and regulations.

NIS 2 Directive

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, on measures for a high common level of cybersecurity across the Union, is probably the most explicit piece of legislation due to imposing direct liability on managing bodies. Under article 20 they are required to approve cybersecurity risk management measures, in addition to overseeing their implementation, and they can be held liable for the entity's infringements. That article also requires specific cybersecurity training for their members and encourages regular training for employees.

In Spain, the Preliminary Bill for a Cybersecurity Coordination and Governance Law, drawn up to transpose this directive, creates the National Cybersecurity Center and establishes the institutional framework and obligations that will implement the NIS 2 requirements.

DORA Regulation

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022, on digital operational resilience for the financial sector, applicable since January 17, 2025, follows the same line of thinking in greater detail. Article 5 imposes ultimate responsibility on the managing body for defining and approving a digital operational resilience strategy, establishing ICT roles and responsibilities, determining technology risk tolerance, and approving, overseeing, and reviewing business continuity and recovery plans. The EBA guidelines adapted to DORA step up the involvement of managing bodies. Furthermore, the obligation to maintain up-to-date information on IT service providers makes oversight of the digital supply chain a governance function.

Artificial Intelligence Act

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence, is particularly relevant due to its cybersecurity and risk management requirements. Article 9 requires providers of high-risk systems to have a continuous and iterative management system throughout the entire life cycle. Article 15 lays down that those systems must be resilient against attempts at unauthorized manipulation. For general-purpose AI models presenting systemic risk, it imposes enhanced obligations, including protection against cyber threats.

Cyber Resilience Act

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024, on horizontal cybersecurity requirements for products with digital elements completes the mesh from a product perspective. It imposes obligations for products with digital components throughout their entire life cycle: security by design and by default, active vulnerability management, and incident reporting. Any company that manufactures or markets connected products falls within its scope, and therefore it applies to a very broad spectrum of European industry.

A clear conclusion can be drawn from a combined reading of these legal acts, and other related ones, such as the GDP: cybersecurity is no longer a matter than can simply be delegated. It is a corporate governance responsibility, and the people in charge can be held accountable.

The digital duty of care: a new fiduciary standard

The accumulation of obligations is not simply the placing of layer upon layer of sector-specific laws and regulations. Taken together, these provisions are shaping a digital duty of care: a fiduciary standard required of directors in relation to cybersecurity, digital resilience, and technology risk management. It is the logical consequence of the legislative convergence described above.

Directors' general duty of care has experienced a gradual sectoral refinement. This was the case with criminal law compliance: the liability of legal entities compelled boards to become involved in risk prevention, approve organizational and management models, create oversight bodies, and allocate

resources to the compliance function. A similar process occurred in relation to anti-money laundering processes, to the point where oversight of the anti-money laundering system became a personal duty of the managing bodies.

Cybersecurity is following the same path, although with one distinctive feature: speed. The transition from generic security obligations, such as those under the GDPR, to a detailed framework of direct responsibilities has taken place in just a few years. Companies and their directors have a much narrower window for adaptation.

This duty has four characteristics that set it apart from other duty of care standards:

a. It is **continuous**, not a one-time event. The dynamic nature of threats demands constant vigilance. It is not enough simply to approve and file a policy: the board must keep track of its suitability in a threat landscape which, by definition, is constantly changing and the directors must stay informed about ICT risks.

b. It is **cross-functional**. Cybersecurity affects the entire organization: supply chain, customer data, production systems, and intellectual property. The managing body needs to have an overall view, rather than one fragmented into departments or business lines.

c. It is **technically demanding**. NIS 2 requires specific training for the members of managing bodies. They cannot be effective at overseeing something they do not understand, and technical complexity cannot justify the board's inaction. Ignorance of technology is no longer a reasonable defense.

d. **Personal liability** cannot be transferred. Members of the managing body can and should rely on internal and external experts, although liability for oversight cannot be transferred. NIS 2 and DORA impose liability on the managing body and provide for personal consequences, including, in certain cases, temporary disqualification for individuals holding management positions.

These provisions converge to shape a standard that goes beyond the generic duty of care expected of an orderly businessperson. As the case law and regulatory practice flesh out its content, it will become established as an independent parameter for assessing the conduct of directors.

Artificial intelligence as a multiplier of cybersecurity risk for the board

While the regulatory landscape already imposes significant requirements, artificial intelligence acts as a multiplier of risk and, therefore, of liability in relation to cybersecurity.

AI has a dual nature. It is a powerful tool for defense, in terms of threat detection, anomaly analysis, response automation, and predictive identification of vulnerabilities, although it is also a sophisticated attack vector: data poisoning, adversarial attacks, deepfakes for social engineering, automated malware generation, or hidden instructions in working papers.

The AI Act addresses this dual role. High-risk systems must achieve an adequate level of cybersecurity and be resilient against unauthorized manipulation. Their risk management system must identify known and reasonably foreseeable risks, including cybersecurity risks, throughout the entire life cycle. For general-purpose models presenting systemic risk, the obligations are even more stringent.

The significance for boards lies in the convergence of these obligations with those in NIS 2, DORA, the CRA, and the GDPR. A company deploying AI must simultaneously monitor the requirements applicable to the system, the data, the ICT infrastructure, and, where relevant, the connected product. All of these provisions may converge on a single technological asset.

This creates an area of heightened liability: the adoption of AI multiplies cybersecurity obligations and raises the standard of care required of the managing body. Implementing AI is not simply a business or innovation decision; it has direct implications on directors' personal liability.

Moreover, the legislation cannot be updated quickly enough to keep up with the pace of change in AI. Lawmakers have preferred principles and risk management over technical requirements that quickly become obsolete. This flexibility places an interpretation responsibility on the board: determining what level of cybersecurity is appropriate for an AI system at any given time.

Practical consequences for managing bodies

The described framework has immediate implications for the organization of boards. Without claiming to be exhaustive, the following are notable:

- Cybersecurity must be a recurring item on their agendas. The board must receive structured information on the status of security, incidents, vulnerabilities, emerging threats, and the degree of legislative compliance, with proportional frequency to the entity's risk profile.

- Training for board members is not optional. They must acquire and maintain sufficient knowledge to understand their organization's risks and critically assess the measures taken. The goal is not to turn them into technical experts, but instead to equip them with the knowledge needed to engage in informed dialog that will enable them to oversee operations effectively.

- Directors' and executives' liability insurance policies must be reviewed. It needs to be checked whether they adequately cover scenarios arising from cybersecurity incidents and whether their coverage is consistent with the penalties and personal liabilities under NIS 2. Inadequate coverage may also reveal a shortfall in the standard of care.

- Organizations of a certain size should create or strengthen specialized technology risk committees. These structures enable the board to fulfill their obligations with the necessary technical depth, without diluting their ultimate liability.

- The digital supply chain takes on a governance dimension. DORA and the CRA require visibility into the risks arising from technology dependence on third parties. Outsourcing IT services does not outsource liability.

- Any decision to adopt AI must include a specific cybersecurity assessment, addressing both legislative compliance and the operational risk that the system introduces into the organization.

Final thoughts

We are facing a paradigm shift: cybersecurity is no longer a technical cost and has now become a fiduciary duty. European legislation has charted a path toward holding governing bodies personally liable in relation to cybersecurity and digital resilience matters.

The digital duty of care is not a theoretical possibility. It is the result of a combined reading of NIS 2, DORA, the AI Act, the GDPR, and the CRA. Any board member of a company subject to these pieces of legislation must be aware that their personal liability is legally defined, is monitored by regulators with the authority to impose penalties and can be enforced in court.

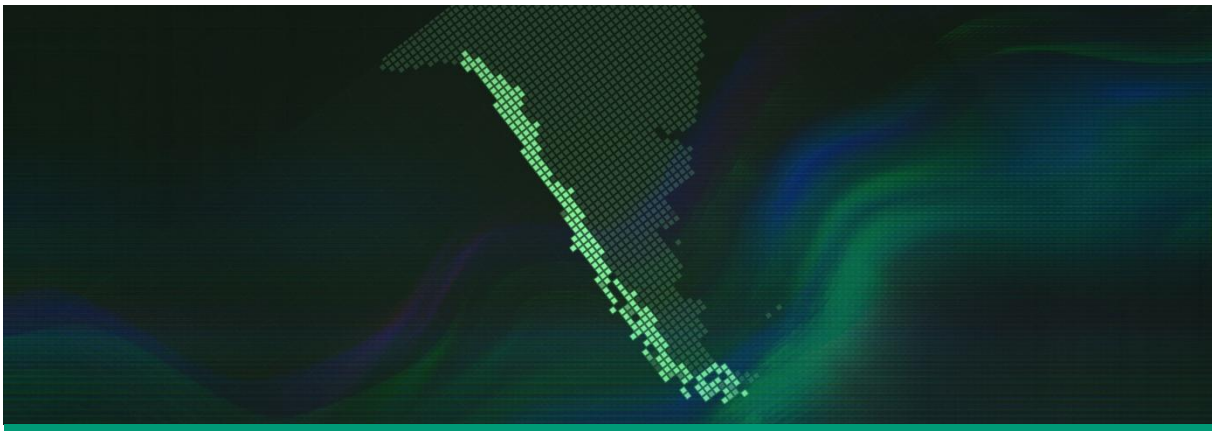
The question is no longer whether a board member should address cybersecurity. The question is how much personal risk they are willing to assume if they do not.

This evolution is reminiscent of the transformation of ESG factors: from a marginal and voluntary issue to a pillar of corporate governance. Cybersecurity and digital resilience are going down a similar path, although at a faster pace and with more immediate and personal consequences: direct penalties, liability for directors, and even temporary disqualification in the most serious cases.

The growing sophistication of cyber risk and D&O policies, with specific types of coverage and exclusions, confirms that this is not simply an academic issue, but instead a market reality that boards must include in their strategy and risk assessment.

In short, cybersecurity has entered the boardroom and is here to stay. Boards that understand this reality will not simply comply with the law: they will protect their organizations, shareholders, and themselves. Blithely delegating responsibility to the IT department is no longer a legally tenable option.

Chile redefines its privacy and cybersecurity framework with new compliance rules and upcoming regulatory changes



Sebastián Barros and Sebastián Hassi

Chile speeds up the transformation of its privacy and cybersecurity framework, with potential changes to adaptation deadlines, new compliance guidelines, and upcoming requirements for the electricity industry. Companies must continue to prepare for a regulatory landscape that is still evolving.

The second half of 2026 has been particularly eventful for Chile's personal data protection and cybersecurity framework. Attention is focused on three developments: (i) the bill approved by the Chilean upper house, now moving to the lower house, pushes back the entry into force of Law No. 21,719 until October 15, 2027; (ii) publication of regulations on models for preventing infringements; and (iii) the preliminary text of the Chilean National Energy Commission's (CNE) technical standard on cybersecurity for the electricity industry. The Chilean National Cybersecurity Agency (ANCI), for its part, issued a procedural adjustment concerning the classification of operators of vital importance and produced implementation initiatives that do not create new obligations.

Personal data protection

Bill proposing to push back the entry into force date of Law No. 21.719 in Chile

On October 28, 2026, the Chilean upper house approved, in the first constitutional reading, a bill amending Law No. 21,719 on the protection and processing of personal data and creating the Chilean Data Protection Agency (Bulletin No. 18,623-07), introduced by a presidential message dated August 31, 2026. After being designated for immediate consideration and reviewed by the Constitution and Finance committees, the bill will now be laid before the lower house for its second constitutional reading. Its main provisions, as approved by the upper house, are:

- **Postponement of entry into force of the law.** The law would take effect on October 15, 2027, instead of December 1, 2026. The date originally recommended in the presidential message was December 1, 2026, the new date was added by the upper house's Committee on Constitution, Legislation, Justice, and Regulations, and the Finance Committee did not add any changes.

- **Agency's executive board.** The number of members is increased from three to five, serving six-year terms, without the option of re-election and with partial renewal every two years, and the quorum for conducting business is raised from two to three.

- **Appointment of the first board.** This must take place by the end of nine months before the law enters into force (currently, six months). The Chilean president will propose, in a single act, the names of two members for six-year terms, two for four-year terms, and one for a two-year term. The upper house must vote on the recommendation as a whole, requiring the affirmative vote of two-thirds of its sitting members. Upon their appointment, the executive board members will be entitled to compensation and must serve on an exclusive basis.

- **Transitional provisions.** The greater amount of fiscal expenditure in the first year will be financed out of the budget of the Chilean Ministry of Economy, Development, and Tourism, and any shortfall will be covered by the Chilean Public Treasury. If, upon publication of this law, there are fewer than twelve months remaining before Law No. 21,719 takes effect, the first appointment must be proposed to the upper house within the following ten days. The text approved by the upper house (a single article with three numbered points and two transitional provisions) does not provide for extension of the written warning regime to all data controllers.

It is essential to make a clear distinction between what the upper house has approved and the law that is in effect. Until the bill completes its passage through the Chilean parliament and is published as law, Law No. 21,719 will come into effect on December 1, 2026, as stipulated in its first transitional article, and the Agency will keep the members established in the provisions in effect. Furthermore, the lower house may introduce amendments to the text.

For companies, uncertainty over the effective date is not a reason for suspending compliance programs. With less than a month to go before the stipulated entry into force date, a prudent stance for companies would be to stick with the compliance schedule, giving preference to the inventory of processing activities, the determination of the legal bases for processing, the review of contracts with data processors, procedures for exercising rights, and the management of security breaches.

Regulations on models for the prevention of infringements

On September 9, 2026, the Chilean Official Gazette published Supreme Decree No. 662 of 2025, issued by the Chilean Finance Ministry, and approving the Regulations on the requirements, methods, and procedures for implementation, certification, registration, and oversight of the infringement prevention models referred to in article 49, which Law No. 21,719 incorporates into Law No. 19,628 (Supreme Decree No. 662 of 2025, issued by the Ministry of Finance, published in the Chilean Official Gazette on September 9, 2026).

The prevention model is voluntary: it may be adopted by any data controller, who may be a public or private individual or legal entity, and it consists of a compliance program. The regulations clarify that its adoption does not alter the general duty of every data controller to prevent infringements and comply with the law. The most notable elements of these regulations are:

- **Minimum content of the program.** It must include, among other elements, a characterization of the data and processing operations (purposes, legal bases, international transfers, retention periods, and automated decisions); a risk matrix identifying the processes with the highest infringement risk, taking into account the severity of penalties; specific prevention procedures; reporting mechanisms; internal penalties, and a reporting channel that ensures the confidentiality of the complainant's identity.

- **Labor and contractual integration.** The internal regulations derived from the program must be expressly included as an obligation in employment and service contracts, including those of top executives, and, where applicable, in the internal rules and regulations governing order, hygiene, and safety.

- **Data protection officer.** The appointment of a data protection officer is mandatory as part of the program's adoption and certification process, although it is not a general requirement for every data controller. The officer must be appointed by the highest authority (such as the board of directors), be independent from management, possess specialized knowledge and sufficient resources, and must report directly to the person who appointed them. The officer may be internal or external, and a corporate group may appoint a single officer if it operates under common standards.

- **Certification, registration, and oversight.** Certification is initiated upon an application submitted by the data subject to the Chilean Agency, it is valid for three years and renewable, and results in registration on the Chilean National Register of Penalties and Compliance, which is publicly accessible. The Agency may oversee certified models, request information, and withdraw certification if, among other grounds, the data controller ceases to meet the requirements.

The main legal effect of the certification model is that it is considered a mitigating factor in relation to any penalties imposed by the Agency. Because the Agency is not yet up and running, the certification process is not yet in operation. However, the regulations allow implementation to begin before entry on the register.

Cybersecurity

Draft Technical Standard on Information Security and Industrial Cybersecurity for the Chilean electricity industry

The Chilean National Energy Commission (CNE) submitted the preliminary wording of the Technical Standard on Information Security and Industrial Cybersecurity for a public comment period between August 28 and October 2, 2026. This is a recommendation: its provisions are not enforceable and could be amended before its final adoption.

Scope of application and relationship to the Chilean Cybersecurity Framework Law. The law would apply to electricity companies, namely, coordinated entities in the Chilean national electricity system (generation companies, transmission companies, distribution companies, storage systems, eligible customers, and small distributed generation facilities (PMGDs), among others, medium-sized system operators, common control centers, and the Chilean National Electric Coordinator. In relation to information security, its requirements would be supplementary and applicable to companies that have not been classified as operators of vital importance (OIV) by ANCI; those classified as OIV would be governed also by Law No. 21,663 and its supplementary regulations. The requirements relating to industrial cybersecurity, however, would apply to all electric utilities and the coordinator. The Framework Law would take precedence in the event of any conflict, and oversight would fall to ANCI in coordination with the Chilean Electricity and Fuels Authority.

Information security. Non-OIV companies would be classified into high, medium, or low impact levels based on objective criteria (for example, more than 100,000 regulated customers for distributors). High-impact companies would be required to implement and certify an information security management system (ISMS) based on the ISO/IEC 27001 standard, with an applicability statement registered with the coordinator; medium- or low-impact companies would be required to implement 36 minimum controls drawn from the ISO/IEC 27001 and ISO/IEC 27002 standards. All companies would have to have an information security policy approved by senior management and an Information Security and Industrial Cybersecurity Unit, with a primary and a deputy officer, to act as the technical counterpart to the coordinator and the authorities.

Industrial cybersecurity. Companies should protect their operational technology environments in accordance with the cybersecurity standard for the electricity industry published by the coordinator in October 2022, based on the NERC-CIP standard. The requirements would depend on the impact level assigned to each network and information system based on the plant where it is located, such as control centers or power plants with a capacity of 300 MW or more. The implementation of complementary standards, such as ISA/IEC 62443 or ISO/IEC 27019, is permitted, and the coordinator would assess the maturity level annually, with the first measurement taking place in 2028.

Proposed time limits. Following publication, the first obligations would have time limits of between one and four months (designation of the Unit, security policy, and scope of the ISMS). The ISMS should be implemented within two years following the approval of the statement of applicability and certified within the following eight months, whereas the minimum controls would have time limits of three or four years depending on the level of impact. The cybersecurity standard would have to be implemented by operating companies within six months to one year, depending on the impact level of the network and information system.

For the industry, the bill confirms that determining OIV status will be key to identifying the applicable rules and that industrial cybersecurity requirements would also apply to OIVs. In view of the recommended time limits, it is advisable to conduct a gap analysis immediately.

Amendment to delegation of the authority to sign at the Chilean National Cybersecurity Agency (ANCI)

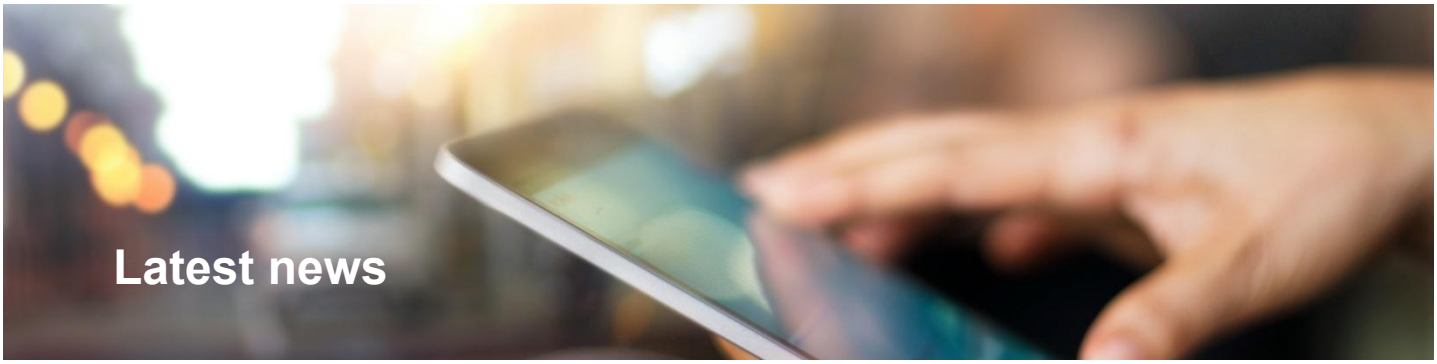
On October 9, 2026, ANCI's Exempt Decision No. 250, dated October 7, 2026 was published, amending Exempt Decision No. 77 of 2025 on delegation of the authority to sign on behalf of the national director. Together with adjustments to purchases and personnel, it includes, among the delegated measures, decisions resolving administrative appeals lodged against measures issued in the OIV classification procedure. The decision does not change either the criteria or obligations applicable to OIVs, although it is relevant for entities challenging their classification, due to determining who signs the decision on their appeals.

Other implementation measures for the Chilean Cybersecurity Framework Law

As part of Cybersecurity Month, ANCI reported that in the first half of 2026 it received 324 reports of incidents with significant impact from essential service providers and OIVs and launched a reporting portal for citizens to report incidents and vulnerabilities, either giving their names or anonymously, using a safe harbor mechanism. This channel does not replace the legal notification obligations of regulated entities. The Agency also announced the first annual Chilean National Cybersecurity Drill, to be held on October 29, 2026, and included the ASPA (Autonomous System Provider Authorization) mechanism into the government's secure connectivity network, making it more difficult for third parties to impersonate the network or divert its traffic to malicious sites.

Principal implications for businesses

In relation to data protection, the statutory entry into force date for Law No. 21,719 is still December 1, 2026, and therefore, the recommended postponement should be treated as a contingency rather than an event to be planned for. Supreme Decree No. 662, already in effect, provides a concrete parameter for organizing internal governance, the risk matrix, and the role of data protection officer. In relation to cybersecurity, companies in the Chilean electricity industry should confirm their status regarding the OIV classification and carry out a preliminary assessment of the impact of the Chilean National Energy Commission's draft standard. Entities subject to the Chilean Framework Law should, for their part, maintain their incident reporting procedures under current provisions.



Latest news

First report received in Spain of a personal data breach carried out through an artificial intelligence agent

The Spanish Data Protection Agency has reported on its blog that it has received the first report of a personal data breach in which the attack was carried out through an artificial intelligence agent based on a language model. According to information provided by the organization concerned, the agent independently carried out various phases of the attack: it identified vulnerabilities, successfully gained access to the system, analyzed the application for further weaknesses, and managed to modify personal data and access invoices. The Agency clarified however that the available information is still preliminary and that it cannot be concluded either that the AI model was compromised or that it had been designed for malicious purposes.

The crucial point for the Spanish supervisory authority is that artificial intelligence appears to have been used as a tool to automate and successfully join up various stages of the attack. Unlike previously known uses of AI in phishing operations, code analysis, or vulnerability scanning, these agents can plan tasks, use tools, interpret results, and adapt their behavior independently to achieve a specific result.

The AEPD emphasized that this notification does not yet mean a statistical trend can be identified, although it is a significant indication that attacks supported by AI agents are no longer simply a theoretical occurrence. From a data protection perspective, the incident highlights the need to explicitly include these types of threats into risk assessments, strengthen vulnerability management, protect credentials and digital identities, and have detection and response mechanisms capable of operating at the speed this technology can allow.

AEPD publishes clarification notice on definitions of accuracy, suitability, and quality of data in processing personal data using AI

In this technical notice, the Spanish Agency starts out from the premise that data quality, as applied to both personal and non-personal data, is broader than the principle of accuracy provided for in the GDPR.

The Agency rejects a narrow view of accuracy based solely on the veracity or up-to-date nature of the data. What matters is whether the data is suitable for fulfilling the purpose of the processing. Depending on each case, this may require attributes such as precision, granularity, frequency of updates, representativeness, or the absence of bias, while in other contexts, exact correspondence with the reality of each individual may not be decisive.

In AI systems based on machine learning, the AEPD emphasizes that quality must also be assessed at the dataset level, since factors such as representativeness or bias may be decisive for the intended purpose, without prejudice to the quality required of individual data points where they have an impact on individuals. Accordingly, a dataset may contain information that is individually correct and yet prove inadequate due to a lack of representativeness or because it incorporates biases that affect the system's operation and results.

The AEPD further acknowledges that certain techniques commonly used in AI development,

such as anonymization, the generation of synthetic data, bias correction, or the statistical imputation of missing values, may introduce data that does not exactly reflect the reality of a specific individual. This does not necessarily imply a violation of the principle of accuracy, provided that the dataset remains adequate to serve the intended purpose and does not have adverse effects on the rights of the data subjects.

Lastly, the Agency emphasizes that quality requirements must be defined using objective criteria and reviewed on an ongoing basis throughout the entire life cycle of AI systems. It also warns that requiring higher quality levels than are actually necessary may conflict with the principle of data minimization, increase costs, and unjustifiably hinder access to data needed for innovation and research.

AEPD warns a company about the necessary safeguards before implementing an artificial intelligence tool to analyze résumés

The Spanish Data Protection Agency has issued a warning to a company that was planning to implement an artificial intelligence tool to analyze résumés, score them, and give preference to candidates, in both hiring processes and internal promotions, even though the tool had yet to be launched.

The Agency acknowledged that artificial intelligence can enhance these processes but highlighted several obligations. The company must apply data protection by design, assess the risks of data processing, and, if these risks are high, conduct a data protection impact assessment before starting. It must also clearly explain to candidates the role the tool plays in their evaluation.

Although the company had specified that the final decision would be made by a person, the AEPD warned that such human intervention is only effective if the decision maker critically assesses the score and does not simply accept the result produced by the tool; otherwise, the right not to be subject to decisions based solely on automated processing could apply. The Agency itself clarified that the warning, provided for in article 58(2)(a) GDPR, is a preventive measure and does not imply that the company has committed any infringement.

AEPD analyzes the risks of exclusion and threats to data protection in the EU digital identity wallet

The Spanish Data Protection Agency has published in its blog the fifth and sixth installments of its series on Regulation (EU) 2024/1183 (eIDAS2), dedicated to the risks posed by European digital identity wallets to inclusion and to protection of their users' personal data.

In the fifth installment, the Agency warns of the risk of exclusion. Making access to the wallet contingent on biometric authentication or specific identity documents, requiring up-to-date devices, or designing complex registration processes without human assistance may exclude people with disabilities, older adults, immigrants, or individuals with low digital competence. Furthermore, although eIDAS2 prohibits denying services for anyone who does not have the wallet, indirect discrimination could occur, such as slower processes or additional requests for information for anyone who does not use it.

The sixth installment analyzes three threats: detection, whereby various actors in the ecosystem could infer sensitive information from application behavior, API responses, or activity logs, even without accessing the data; data breaches, which could have a very severe impact where identification documents or biometric data are stored centrally or for extended periods; and over disclosure of personal data beyond what is strictly necessary.

To mitigate these risks, the AEPD recommends implementing privacy by design through selective disclosure of attributes, local processing of information, the use of pseudonyms, and advanced cryptography mechanisms.

AEPD publishes recommendations on best practices for use of smart sunglasses with built-in cameras and microphones

The Spanish Data Protection Agency has published an article analyzing the privacy implications arising from the use of smart sunglasses equipped with cameras and microphones, which have gained increasing presence on the market in recent months and users can use to capture images, sound, and other personal data in a way that is barely noticeable to anyone close by, unlike conventional cameras or cell phones.

In its publication, the Agency recommends using these sunglasses with the same caution as you would a camera or cell phone, transparently informing others when you are about to record, paying special attention to audio recording, and limiting recordings to what is strictly necessary. It also advises using the appropriate privacy and security settings on devices, reviewing what additional data these devices collect, such as location or metadata associated with recordings, complying with existing legal restrictions in certain locations, and deleting recordings when they are no longer needed.

This publication is of interest in the context of the growing popularity of these devices, as their use by individuals may involve the processing of personal data subject to the GDPR and raises questions regarding the capture of images in public and private spaces, the recording of conversations, and the potential application of video surveillance regulations.

Compatibility between blockchain and personal data protection under the GDPR

The European Data Protection Board (EDPB) has approved new guidelines on the processing of personal data using blockchain technologies, a document drafted under the leadership of the Spanish Data Protection Agency (AEPD). The guidelines aim to provide legal certainty to organizations using this technology and to clarify how they can reconcile its technical characteristics with the requirements of the GDPR.

The EDPB acknowledges that the main legal tension stems from the very nature of blockchain technology, which is based on distributed and immutable ledgers, a feature that may conflict with fundamental data protection principles such as storage limitation, data minimization, and the right to erasure. However, the guidelines conclude that the use of this technology may be compatible with the GDPR provided that an appropriate architecture and privacy-oriented governance are adopted.

Among the most relevant criteria, the EDPS advises against storing personal data directly on the blockchain and recommends that identifying data remain off-chain, and that the information recorded on the chain should be limited to cryptographic proofs or technical references that reduce the risk of identifying individuals. It also emphasizes the need to apply privacy-by-design and privacy-by-default measures, by including data minimization, pseudonymization, and encryption mechanisms from the earliest stages of the project.

The guidelines also emphasize that the data subjects' rights provided for in the GDPR, including the rights of access, rectification, objection, and erasure, remain fully applicable in blockchain environments. To this end, various technical solutions are considered to ensure the effective anonymization or irreversible de-identification of information where it is necessary to fulfill these rights.

Finally, the EDPB considers that data processing carried out via blockchain typically presents high risks associated with the replication of information, the decentralization of the network, and potential international data transfers. For this reason, organizations must conduct a data protection impact assessment (DPIA) before implementing such solutions where there are significant risks to the rights and freedoms of individuals.

The adoption of these guidelines marks a significant milestone in application of the GDPR to decentralized technologies.

Publication of the AI Omnibus Regulation, which simplifies requirements and defers certain obligations provided for in the European AI legislation

Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026, amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) was published in the Official Journal of the European Union on July 8, 2026. This is a European legislative initiative aimed at simplifying certain regulatory obligations arising from Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence (the AI Act), in order to strengthen European competitiveness in the field of artificial intelligence. The measure is part of a broader regulatory simplification strategy promoted by the European institutions to cut red tape and facilitate the adoption of digital technologies.

One of the main changes involves extending certain implementation time limits and revising a number of documentation requirements originally laid down for providers and developers of AI systems. The goal is to enable a more gradual adaptation to the new regulatory framework, particularly for small and medium-sized enterprises and startups.

The regulation also introduces measures aimed at protecting the interests of minors as well as protecting privacy, simplifying certain reporting requirements, and removing the general AI literacy requirement that had been imposed on all operators, among other measures. The Commission believes that these amendments will make it possible to preserve the AI Act's objectives of safety, transparency, and the protection of fundamental rights without imposing disproportionate burdens on economic operators. For more information see this article.

European Commission fines Google €890 million for non-compliance with the Digital Markets Act

The European Commission has imposed fines totaling €890 million on Google, in its gatekeeper role, for breaching the Digital Markets Act (Regulation (EU) 2022/1925). The violations relate to self-preferencing its own services in search results and putting in place restrictions on app developers in relation to informing users about offers available outside the platform.

On the first violation, the Commission concluded that the operator gave preferential treatment to its own services, including shopping, hotels, transport and sports results, over those of competitors. According to the European authority, these results were given a more prominent position, with visual elements and features not available to third parties, thereby breaching the obligation to apply transparent, fair, and non-discriminatory criteria required by the DMA. The Commission imposed a €460 million fine for this conduct.

The second decision concerns anti-steering restrictions applied through an app store. The Commission found that the operator prevented developers from freely informing users about the existence of alternative or cheaper offers outside the platform and restricted their ability to contract directly with users through other channels. It also determined that the fees charged for certain customer conversions exceeded what is permitted under the DMA. An additional €430 million fine was imposed for this violation.

The decision reinforces the principle that gatekeepers cannot use their position to give preferential treatment to their own services or restrict access by businesses and consumers to competitive alternatives.

EDPB publishes Guidelines 04/2026 on the imposition of administrative fines in relation to other corrective powers under the GDPR

The European Data Protection Board (EDPB) has published Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR, along with the final version of its guidelines on the interplay between the Digital Services Act (Regulation (EU) 2022/2065) and the GDPR.

According to Guidelines 04/2026, data protection authorities should follow a five-step methodology when deciding whether to impose an administrative fine. The document provides an overview of the corrective powers of national authorities and explains their purpose, scope, and how they relate to one another. These corrective measures include warnings, reprimands, orders, limitations (including bans), and the withdrawal of certification.

The guidelines are useful for data controllers and processors, as they help anticipate the reasoning that the supervisory authorities will apply when choosing between a fine and other corrective measures, and they reinforce consistency in how the GDPR is applied across the various member states.

New European guidelines on data anonymization and mass data extraction for training artificial intelligence models

The European Data Protection Board (EDPB) has adopted Guidelines on data anonymization and web scraping in the context of generative AI.

In relation to anonymization, the EDPB has clarified when a dataset can be considered properly anonymous for the purposes of the GDPR. Data is anonymous only when it no longer allows for the direct or indirect identification of an individual. To test the effectiveness of anonymization, it proposes three fundamental criteria: no isolation of individual records, no linkage of data across different sources, and no inference of a person's identity. If all three requirements are met, the data may be considered anonymous.

In relation to web scraping for generative AI, the EDPB notes that the automated extraction of data from internet sources constitutes processing subject to the GDPR when it involves personal data. Organizations must have a valid legal basis, comply with the principles of transparency, purpose limitation, data minimization, and accuracy, and preferably use reliable and verified sources for training AI models. It further emphasizes that the processing of special categories of data continues to be prohibited generally unless a specific exception provided for in the GDPR applies.

Taken together, these initiatives reinforce the European position that the development of emerging technologies - AI, advanced anonymization, and blockchain - must ensure the effective protection of individuals' fundamental rights and privacy.

French data protection authority issues recommendations on the processing of location data from connected vehicles

The French data protection authority (*CNIL - Commission nationale de l'informatique et des libertés)* published recommendations, on June 30, 2026, regarding the use of personal location data in connected vehicles, aimed at manufacturers, fleet managers, telematics providers, and data aggregators.

The guidance classifies location data as highly personal data, subject to the GDPR and Directive 2002/58/EC, because it reveals movements, frequently visited places, and areas of interest. All processing must pursue a specific, explicit, and legitimate purpose. Each party must identify its role: controller, joint controller, or processor. Where consent is required, it must be obtained prior to processing and must be freely given, specific, informed, and unambiguous. Furthermore, consent must be able to be withdrawn as easily as it was given.

On a technical level, the CNIL recommends:

1. minimizing data by retaining, for example, only the last location where that is sufficient;
2. limiting retention periods;
3. pseudonymizing and, where possible, anonymizing data as soon as this can be done, preferably within the vehicle itself;
4. encrypting data in transit and at rest;
5. managing access permissions with periodic reviews and logging access;
6. segregating data by customer and by purpose;
7. conducting a data protection impact assessment where there is a high risk.

The guide also requires transparent reporting on several channels (contract, in-vehicle display screen, QR codes, and privacy policy). Additionally, the means for exercising rights of access, rectification, erasure, and portability must be provided.

ENISA launches Cyber Resilience Act single reporting platform for vulnerabilities and serious incidents

The European Union Agency for Cybersecurity (ENISA) has launched the initial operational capability of the *Single Reporting Platform*, the single reporting platform provided for in the Cyber Resilience Act (Regulation (EU) 2024/2847). This tool is designed to simplify compliance with the reporting obligations provided for by the regulation, by allowing manufacturers of products with digital components and those responsible for open-source software projects to report once, which will then be forwarded to the relevant competent authorities.

The launch of this platform marks the beginning of the implementation of one of the most significant obligations under the Cyber Resilience Act: the reporting of actively exploited vulnerabilities and serious security incidents affecting digital products. Through this, the European Union seeks to improve coordination among authorities and strengthen the response capacity to threats that could compromise the security of connected products and digital services.

The creation of a single reporting mechanism is also aimed at reducing administrative burdens on obliged entities and promoting more efficient and consistent management of information on cyber incidents in the European market. This initiative represents one of the first operational milestones of the Cyber Resilience Act, a regulation that introduces cybersecurity requirements throughout the entire life cycle of digital products and seeks to raise security standards for devices and software marketed in the European Union.

EDPB calls on European Commission to establish a legal basis for the sharing of information between regulatory authorities with different powers

The European Data Protection Board has called on the European Commission to establish a specific legal basis for the sharing of information between regulatory authorities with different but adjacent powers, a process known as cross-regulatory information sharing. Its goal is to facilitate the transmission of relevant information, including confidential information, and to improve the coordinated enforcement of European Union legislation in an increasingly interconnected regulatory environment.

According to the EDPB's publication, this request responds to the growing interaction among the various European regulatory frameworks affecting the digital environment, including data protection, the regulation of artificial intelligence, digital services, digital operational resilience in the financial sector, and cybersecurity, areas in which effective oversight often requires cooperation between authorities operating under different regulatory regimes and which, at times, lack a clear legal basis for sharing information obtained in exercising their supervisory functions.

The EDPB also highlighted the need to strengthen cooperation among data protection authorities themselves in light of the increasing volume and complexity of cases particularly those related to artificial intelligence by promoting the sharing of resources and joint

actions to ensure a more effective and consistent application of the GDPR.

Publication of the conclusions of a group of more than 100 experts on competitiveness, sovereignty, and security in the field of cutting-edge AI

The European Artificial Intelligence Office, a body attached to the European Commission with responsibilities for overseeing the Artificial Intelligence Act, has published a report containing the findings of more than 100 experts on how to enhance the European Union's position in the development of cutting-edge AI.

Among their key recommendations is the need to improve conditions for attracting investment and talent, particularly by scaling up computing capacity and the energy infrastructure required to develop and train advanced artificial intelligence systems. The experts also pointed to the importance of providing greater legal clarity in areas such as data protection and copyright, which is decisive for the questions raised about the legal basis for processing personal data and the reuse of protected content in connection with training advanced AI models.

The report placed the spotlight on European technological sovereignty, underlining that the European Union must be able to access, use, and benefit from the most advanced AI models, including those developed outside its borders. It states that it is essential to derive leverage from assets such as the European market size, the EU's regulatory heft, and its industrial strength, as well as to strengthen collaboration with trusted international partners.



Decisions

Uber fined for automatically deactivating its drivers' accounts through fully automated decisions

On August 21, 2026, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) fined Uber €824,990,000 for making fully automated decisions regarding its drivers. Between 2018 and 2022, the company used software to track drivers' driving behavior and customer reviews. If the software identified a suspicion of fraud or customer reviews were too low, drivers' accounts were automatically deactivated temporarily or, if the reviews were persistently low, permanently. In the deactivation period the driver stopped receiving any income via the platform and no human intervention took place at any time

From a data protection standpoint, the Dutch authority identified two breaches. The first a breach of the prohibition on decisions based solely on automated processing, set out in article 22 of the GDPR: a decision with consequences as severe as depriving someone of income cannot be made by a computer system alone, and must first be reviewed by a human. The second was that Uber did not sufficiently inform its drivers about these automated decisions.

The decision highlights the increasing scrutiny by supervisory authorities of the use of algorithms in the management of digital platform workers, and the importance of ensuring genuine human involvement and adequate information when automated decisions have a significant impact on individuals.

Google fined for processing its users' location data without a valid legal basis or sufficient transparency

On September 21, 2026, the Data Protection Commission of Ireland (DPC), in its role as the Lead Supervisory Authority for Google, announced its final decision against Google Ireland Limited. The authority launched an own-volution inquiry in 2020, after receiving complaints from several consumer organizations, including the European Consumer Organization (BEUC). It focused on the processing of location data in three of Google's features – "Web & App Activity", "Location History" and "Location Accuracy", between May 2018 and February 2020.

The Irish authority found that four breaches had taken place: the first concerned the principles of lawfulness and fairness, because the processing of location data in web and app activity and location history lacked a valid legal basis and was not carried out in a manner that was fair to the user. The second related to proactive accountability: regarding the location accuracy feature, Google was unable to demonstrate compliance with the GDPR, underscoring that mere compliance is not sufficient - it must also be demonstrable. The third was transparency, since the information provided regarding the three features did not make it clear to users what was being done with their location data. The fourth breach concerned the limitation on retention periods, since the data was stored for longer than necessary.

As a result, the Irish authority imposed fines totaling €403 million due to the infringement of articles 5, 6, 12 and 13 of the GDPR and ordered Google to bring its data processing into line within six months.

AEPD fines a mutual society €2.4 million for a security breach that compromised genetic and health data

The decision forms part of a penalty proceeding initiated against a U.S. company that conducts genetic testing and genetic data analyses, following a security breach that affected 2,642 customers residing in Spain. The incident stemmed from a cyberattack in which third parties accessed user accounts through credentials that had previously been compromised on other services. As a result, particularly sensitive information was revealed, including genetic and health data, as well as data that revealed the ethnic origin of those affected. Furthermore, some of the information was posted on internet forums and offered for sale on the dark web.

In its decision the AEPD concluded that article 5.1.f) of the GDPR had been infringed because security measures appropriate to the risk posed had not been implemented. The Agency underscored that access to the accounts was obtained using only a username and password, that multi-factor authentication was optional and that there were insufficient limits or checks on mass access to and downloading of data. The AEPD imposed a €2,000,000 fine.

Furthermore, the Agency considered that article 33 of the GDPR had been infringed due to the delayed notification of the breach. Although the entity had sufficient evidence that a security breach had occurred on October 5, 2023, it did not notify the AEPD of the breach until October 17, far exceeding the maximum 72-hour deadline set out in the GDPR. An additional €400,000 fine was imposed for the breach.

Telecommunications operator fined for a security breach suffered by its provider

The AEPD has fined a telecommunications operator for a data breach that occurred in the systems of one of its suppliers. The supplier had developed the operator's WIFI service application and was processing the operator's customer data through the service. In November 2023, the provider suffered a cyberattack in which a third party gained access to its systems using legitimate credentials, revealing the email addresses and, in some cases, the first and last names of thousands of customers, data that ended up being sold online.

The operator argued that the breach had occurred in the supplier's systems and that it had signed a data processing agreement with the supplier that included security instructions. In its decision, the AEPD rejected the argument for two reasons: first, the data controller is liable for the actions of its processors, unless they have decided the purposes and means of the processing, which did not occur in this case. In addition, the controller is responsible for ensuring that the processor complies with the rules and must not simply impose formal obligations. Second, when the breach occurred, there was no valid agreement in place: it was signed in September 2024, nearly a year after the attack, although it stated that it had been in force since December 2022. In the Agency's view, this retroactive effect is invalid, as the data processing agreement must be signed in writing before the processor starts processing data.

As a result, the AEPD imposed three fines: a €500,000 fine for violating the principle of integrity and confidentiality under article 5.1.f) of the GDPR; a €150,000 fine for failing to implement appropriate security measures in accordance with article 32 of the GDPR; and a €100,000 fine for not having signed the data processing agreement as required by article 28 of the GDPR when the breach took place.

Used car dealer fined for a personal data breach, providing insufficient information on retention periods and lack of security measures

The AEPD has imposed fines totaling €680,000 on a company in the used car industry after verifying that three breaches of the GDPR had taken place following a personal data breach that led to a loss of confidentiality and affected a significant number of data subjects.

The AEPD found that article 5.1.f) of the GDPR, regarding the principle of integrity and confidentiality had been breached, on the grounds that the security measures in place before the breach were insufficient to prevent it or, at least, mitigate its effects. A €400,000 fine was imposed for this infringement. An

infringement of article 13 of the GDPR was also found to have taken place, on verifying that the information provided to non-qualified customers regarding the retention period for their data was insufficient, because it did not adequately specify that period. The penalty for this violation amounted to €30,000. Lastly, the Agency found that article 32 of the GDPR had been breached, noting that the company had not taken adequate measures to ensure an appropriate level of security with respect to the blocked personal data of former potential customers. A €250,000 fine was imposed for this infringement.

On top of the financial penalties, the company was ordered to evidence, within one month of the ruling becoming final, that its privacy policy provided more detailed information on the retention period, particularly for unqualified customers and to evidence, within four months, that it has adopted the appropriate measures to comply with the GDPR's security requirements regarding the blocking of data.

Electricity retailer fined for inadequate permission settings and deficiencies in access control

The AEPD has fined an electricity retailer following a security incident in which third parties used credentials stolen from an authorized supplier to access customers' identifying, contact, banking, contractual, and billing data. Although the initial access was gained using legitimate credentials, the compromised user had been erroneously assigned permissions that allowed them to view the entire customer portfolio, instead of being limited to the information necessary for the requested commercial activity.

The Agency determined that the unlawful use of credentials did not exempt the retailer from liability. An incorrect configuration of the roles enabled the incident to expose information that the provider was not authorized to access, which demonstrated a serious lack of diligence. It also identified additional deficiencies in access management, such as the shared use of a single account by approximately 120 workers, the lack of individual traceability, the absence of expiry dates for credentials, and public exposure of the applications without sufficient additional restrictions.

The AEPD distinguished between the violation of the principle of integrity and confidentiality under article 5.1.f) of the GDPR due to the actual access to the data and the separate breach of article 32, regarding the lack of security measures appropriate to the risk. It also refused to stay the proceedings because of the criminal investigation into the attack, as the data controller and alleged perpetrator of the offense concerned different parties.

As a result, it imposed a €400,000 fine for a breach of article 5.1.f) and a €275,000 fine for a breach of article 32 of the GDPR, in addition to ordering the adoption of corrective measures and proof of their implementation within three months.

Irish health service fined €645,000 due to failings in the retention and storage of paper medical records

The Irish Data Protection Commission fined the Irish Health Service Executive €645,000 following an inquiry into the retention and storage of personal data contained in paper records. The inquiry commenced following several security breaches involving unauthorized access to medical records stored in former psychiatric hospitals and was expanded to include inspections of twelve storage facilities across the country.

The Irish authority found that the Health Service had failed to meet its obligations in several areas. Regarding security, adequate security and document management controls were not in place; inspectors found records damaged by mold, water, and animal excrement, as well as documents stored in disused bathrooms, shipping containers and derelict buildings. Regarding retention, personal data were retained beyond the period where they should be retained, breaching the GDPR's principle of data storage limitation. Furthermore, some data breaches were not reported within the mandatory 72-hour deadline and certain data subjects were not informed of the breaches affecting them.

In addition to the fine, the authority ordered the Health Service to carry out a complete audit all of its facilities where it stores and retains paper files, improve its management system for tracking and tracing the location of all paper

records, remove paper records that are not fit for purpose and move them to appropriate facilities. The decision underscores that data protection obligations apply regardless of whether information is stored in digital or paper format and highlights the importance of institutional accountability and retention periods.

Bank fined €510,000 for requiring excessive inheritance documentation and failing to provide adequate information about data processing

The AEPD has fined a banking institution for the design of its inheritance management procedure, after finding that it required heirs to provide a complete deed of acceptance, partition and distribution of the estate, thereby allowing access to financial information unrelated to the banking products being processed.

The authority concluded that this practice infringed article 25 of the GDPR (data protection by design and by default). According to the decision, the institution's internal procedure did not adequately respect the principle of data minimization, as it was configured in a way that involved processing financial information about the deceased and the heirs that was not necessary to manage the banking products affected by the inheritance. The AEPD emphasized that the regulations and criteria of the Bank of Spain allow, in certain cases, for the division of the estate to be evidenced via private documents signed by the heirs, without the need to provide a complete public deed.

Furthermore, the AEPD found that article 13 of the GDPR had been breached because the bank had failed to demonstrate that it had provided the data subjects with the required information regarding the processing of their personal data when it was collected. It did not consider the mere existence of a privacy policy published on the bank's website to be sufficient either, as there was no evidence that such information had actually been made available to the data subjects.

As a result of these findings, a €500,000 fine was imposed for the breach of article 25 and another €10,000 fine for the breach of article 13. The breach of article 30 of the GDPR, on records of processing activities that had been investigated initially was ultimately dismissed. After the company elected voluntary payment, the fine was reduced to €408,000.

Telecommunications operator fined €900,000 for security and oversight deficiencies relating to its processors following two ransomware attacks

The AEPD has fined a telecommunications operator in two separate proceedings for two personal data breaches resulting from ransomware attacks against systems managed by external providers acting as data processors. In both cases the Agency concluded that the operator had failed to implement security measures appropriate to the risk, in breach of article 32 of the GDPR.

In the first case, analyzed in this decision, the attack occurred in November 2023 on a platform maintained by a technology provider and affected the confidentiality and availability of the data of 724,733 customers. The attacker gained access through a generic account with a weak password and no multi-factor authentication on a virtual private network (VPN) that was part of the operator's own infrastructure and the Agency therefore considered this to be a structural deficiency attributable to the controller. Although the AEPD initially held that article 5.1.f) of the GDPR had been breached, it ultimately classified the facts as a single violation of article 32 and imposed a €500,000 fine.

In the second case, set out in this other decision, the breach originated in the systems of a processor that provided incident management services and affected over 486,000 private customers and thousands of authorized corporate users. Although some of the information was encrypted, phone numbers and other identifiers remained accessible. The Agency found a lack of diligence in the provider's oversight, as there had been a recent history of cyberattacks and known critical vulnerabilities that had not been corrected and it imposed a €400,000 fine, although it considered the corrective measures adopted after the incident to be a mitigating factor.

Both rulings applied the same criterion: hiring a data processor and establishing security

obligations for them in an agreement does not exempt the controller, who must verify through effective audits and controls that these measures are actually being implemented. Only when the data processor processes the data for its own purposes, in accordance with article 28.10 of the GDPR, can liability be transferred to it.

Security company fined for using a 902 number to exercise data protection rights on CCTV information signs

The AEPD has fined a private security company for including the statement "right of access and objection via the phone number indicated" on certain CCTV information signs, directing data subjects to a 902 number. The complaint was filed by the consumer association FACUA-Consumidores en Acción, which argued that this system hindered the exercise of rights recognized under the data protection legislation.

The Agency noted that article 12 of the GDPR requires data controllers to facilitate the exercise of data subjects' rights and that the means provided must be easily accessible. Although the entity provided free alternative channels through its website and its data protection officer, the AEPD held that the existence of other channels did not eliminate the legal significance of the message on the sign, which expressly directed data subjects to a premium-rate phone number to exercise their rights of access and objection.

The ruling highlights that 902 numbers entail a higher cost for users than a standard call and, as a general rule, are not included in flat-rate phone plans. As a result, the Agency concluded that directing data subjects to this type of number does not constitute a means that effectively facilitates the exercise of rights under the GDPR. It also considered particularly significant that the practice had continued for years and involved a very large number of information signs installed by the company.

The AEPD therefore held that article 12 of the GDPR had been breached and imposed a €100,000 fine, in addition to ordering the replacement of the signs concerned with others that comply with the data protection legislation within twelve months.

AEPD fines the RFEF €100,000 for collecting unnecessary data for the registration of a minor

The AEPD has fined the Spanish Football Federation for requiring both a certificate of registered domicile and school certificates to register a minor who was born and resides in Spain but holds foreign nationality. The documentation was requested to prove that the player had resided continuously in Spain for at least five years, a requirement set out in the International Federation of Association Football (FIFA) regulations on the registration of minors.

The Spanish Football Federation (RFEF) argued that both documents were necessary to prove actual residence and prevent situations of exploitation or uprooting of minors. However, the Agency noted that FIFA's official and binding guidelines consider the residence certificate and school certificates to be alternative, not jointly required, means of proof. Therefore, if either of them is sufficient to prove continuous residence, requiring both implies collecting additional data without a separate purpose that justifies their processing. The AEPD added that the communications provided regarding an alleged practice by FIFA did not prove that both documents should be systematically required.

Consequently, the Agency found that article 5.1.c) of the GDPR had been infringed, due to a breach of the principle of data minimization and imposed a €100,000 fine. It also ordered the RFEF to adapt, within two months, the processing carried out in these registration procedures in order to limit the data collected to what is strictly necessary.

AEPD notes that blocking data does not exempt an organization from complying with the right of access

In its ruling on case PD-00073-2026, the AEPD makes a number of suggestions regarding the right to erasure and its interplay with the obligation to block data as provided in the Spanish data protection law (LOPDGDD), as well as on the right of access.

Although this does not represent a radical change in the supervisory authority's

understanding of these concepts, it is a ruling worth reviewing, as it clarifies a number of concepts open to debate, such as the implications of data blocking and how it interplays with the two aforementioned rights.

Regarding the right to erasure, the AEPD states that the erasure of data must be carried out through blocking. Consequently; exercising the right to erasure does not necessarily entail the physical deletion of the data at that precise moment. In relation to the right of access, the AEPD notes that "when the right of access is exercised, it is unacceptable to leave the exercised right of access unanswered simply because the requested personal data is blocked." In other words, when the right of access is exercised, the blocked data must be consulted, and, where appropriate, provided as part of the exercised right.

Once again, while these issues are not particularly novel, given the frequent debate sparked by these concepts, this ruling is highly important, due to containing the AEPD's most recent known position on the matter.

University commits infringement by revealing that a candidate had been the victim of gender-based violence in an admissions process

The AEPD has ruled that a Spanish university committed an infringement by including, in the decision on a complaint filed during an admissions process, information that allowed a candidate to be identified as a victim of gender violence. The decision was notified to another applicant involved in the same procedure after the two complaints were joined.

The university argued that the disclosure was covered by the right of access to the case file and by the need to adequately justify the decision made in the public recruitment process. However, the Agency considered that identifying the candidate along with the express reference to her being a victim of gender-based violence went beyond what was strictly necessary to guarantee the right of defense of the other interested parties.

The AEPD noted that the right of access to the case file in administrative proceedings is not absolute and must be balanced with data protection principles. In particular, it emphasized that the principle of data minimization requires limiting the information disclosed to information that is adequate, pertinent and necessary for the intended purpose, with anonymization or pseudonymization techniques to be used where particularly sensitive data is involved.

Consequently, the Agency found that article 5.1.c) of the GDPR had been infringed, due to a breach of the principle of data minimization and ordered the University to adopt, within three months, the necessary measures to ensure compliance with this obligation in its procedures.

Company fined for failing to implement sufficient security measures on a bulletin board regarding workers included in a collective layoff

The AEPD has fined a Spanish company for failing to comply with the security obligations set out in article 32 of the GDPR by making a bulletin board available to the works council that lacked adequate protection measures. The action was taken after it was verified that the minutes of a collective layoff proceeding had been posted on the bulletin board, together with an attachment containing the personal data of the included workers , including their names, national ID numbers, social security numbers, dates of birth, and other employment-related data.

The Agency distinguished between the liability arising from the specific publication of the documentation – attributable to the person who physically placed it on the bulletin board – and the company's liability for failing to implement adequate technical and organizational measures regarding the publication system itself. In particular, it was found that the bulletin board did not have a lock or access control, there were insufficient measures to restrict who could publish or remove documents and there was no evidence of adequate training or instructions in relation to data protection for those authorized to use it.

The AEPD noted that article 32 of the GDPR requires that a risk assessment must be carried out and appropriate security measures must be adopted in light of the nature and purpose of the

processing. In the workplace, this involves ensuring that only authorized individuals can manage published content and that the processing of personal data is carried out in accordance with data protection principles.

Consequently, the Agency determined that article 32 of the GDPR had been breached due to the failure to adopt adequate technical and organizational measures and imposed a €15,000 fine on the company – lower than the amount initially proposed, due to certain mitigating factors being identified relating to the conditions of access to the workplace and the company's circumstances.

AEPD fines a medical imaging diagnostics provider for failing to have adequate measures in place to detect security breaches

The decision was issued in a penalty proceeding initiated against a company engaged in providing diagnostic imaging services following a security breach that compromised the personal data of 1,352 patients. The incident stemmed from a cyberattack in July 2024, during which unauthorized third parties gained access to the company's systems and exfiltrated patient information, including health-related data, a special category of data under article 9 of the GDPR.

In its decision, the AEPD concluded that, regardless of the fact that the attack's entry vector could not be determined with certainty, the organization did not have technical and organizational measures in place that were appropriate to the risk posed by the processing, as required by article 32 of the GDPR. The Agency highlighted in particular the deficiencies in the mechanisms for the early detection of security incidents, since the organization was unaware of the breach until it received the extortion messages sent by the actual attacker, which demonstrates a lack of monitoring systems capable of proactively identifying anomalous access or data exfiltration.

Consequently, the AEPD held that article 32 of the GDPR to had been breached, because an adequate level of security was not ensured when processing special categories of data, the exposure of which poses a high risk to the rights and freedoms of the data subjects concerned. As a result, the Agency handed down a €30,000 fine, in accordance with article 83.4 of the GDPR.

EDPB rejects the notion that a complaint regarding cookie banners can be dismissed on the grounds that it is part of a coordinated campaign

The matter stems from a complaint filed by NOYB (None of Your Business), an Austrian organization that specializes in promoting compliance with the GDPR through strategic complaints, against the Belgian public broadcaster regarding the operation of its cookie banners. The Belgian data protection authority proposed dismissing the complaint, on the grounds that there had been an abuse of the right to file a complaint, since the complaint formed part of a campaign organized by NOYB and had been prepared as part of a coordinated strategy to challenge cookie banners. However, the Austrian authority objected to this conclusion and argued that the complaint should have been assessed on the merits.

In its decision, the EDPB concluded that no abuse of rights had been evidenced. It noted that, according to CJEU case law, both an objective and a subjective element must be present to establish such an abuse. In this case, although the organization played an active role in identifying potential infringements and preparing the complaints, the EDPB considered that such action was consistent with the purpose of article 80(1) of the GDPR, which allows specialized organizations to represent data subjects in data protection matters. Furthermore, there is no evidence that the complainant or the organization sought any undue advantage other than ensuring compliance with the regulations.

Consequently, the EDPB ordered the Belgian authority not to dismiss the complaint and to examine the case on its merits, thus upholding the legitimacy of complaints filed by entities that specialize in data protection and limiting the possibility that supervisory authorities will reject them merely because they form part of coordinated GDPR compliance campaigns.

Notary's office fined for providing a client with a cadastral certificate containing protected data of a third party without a legitimate basis

The AEPD has imposed a €2,000 fine on the owner of a notary's office following a complaint by an individual who had received a letter from one of the notary's clients, accompanied by a descriptive and graphic cadastral certificate. The letter proposed that the individual sign a document acknowledging that she was not the owner of a property so that it could be removed from the cadaster and registered in the client's name. The certificate identified the complainant as the owner of the plot and included her first name, last name, and address, data that is protected under cadastral regulations.

During the investigation, the Directorate General for the Cadaster confirmed that the certificate had been obtained by the notary's office for information purposes. The notary's office acknowledged that it had obtained the certificate at the request of its client, who provided the cadastral reference number so that her son could negotiate with the owner the purchase or lease of the property and that it subsequently delivered the certificate, which contained the complainant's protected data, to the client.

The Agency concluded that, although the notary's office could access protected cadastral information if legal conditions were met, providing the certificate to the client for a potential real estate transaction was neither justified nor had a legitimate basis in accordance with article 6.1 of the GDPR. The client used the data to go to the complainant's residence and send her a letter, which constitutes a violation of article 6(1) of the GDPR, as specified in article 83(5)(a) of the same text.

Furthermore, the notary was ordered to demonstrate, within three months, that the necessary measures had been taken to ensure compliance with article 6.1 of the GDPR in all of its personal data processing operations.

Municipal regulated parking company fined for recording its employees' conversations using a walkie-talkie app without informing them

The ruling imposes a penalty on the municipal company that manages the regulated on-street parking service in Palma (the so-called "blue zone") for failing to process its employees' data in a fair and transparent manner, in breach of article 5(1)(a) of the GDPR. In 2022, parking attendants complained that the system for reporting emergencies was complicated, so the company decided to test an alternative app that functions as a walkie-talkie on a cell phone. The app was installed on the employees' personal digital assistants (PDAs) and was activated on 92 of them. In November 2022, it came to light that the app had recorded a conversation among several employees during their break and that this recording was accessible to area managers. Following a complaint by the labor unions, the company uninstalled the app and deleted the recordings a few days later.

The company submitted in its defense that the app was only in the testing phase and that it never actually used the recordings, that it had verbally informed the workers when activating the app and that it could not disclose the risks because the app did not have a technical manual. The AEPD rejected all three arguments in its ruling. Firstly because recording a conversation already constitutes data processing, even if the recording is not used subsequently. Secondly, the company did not provide evidence of what information it had disclosed when activating the app, it failed to inform those who had installed but not activated the app and its privacy policy made no mention of the recordings. Third, precisely because the tool was in the testing phase, the company was required to exercise the utmost transparency and warn that it could malfunction and affect employees' rights; by acknowledging that it was unaware of the risks, it admits that it installed the app without informing employees accordingly. The imposed fine totaled €40,000.

Driving school network fined for a security breach that exposed the data of more than 264,000 people after ignoring warnings from the police

The ruling was issued in a disciplinary proceeding initiated against a network of driving schools with franchises throughout Spain, following a security breach. The Cyberattacks Team belonging to the Spanish National Police Force's Central Cybercrime Unit discovered that a database belonging to the company was being sold online, containing information on students and employees, such as first and last names, national ID numbers, phone numbers, email addresses, and home addresses. A total of 264,435 people were affected, including some underage students. A sample of the data was posted on a cybercrime forum as proof that the theft had actually occurred.

The company ignored warnings both from a cybersecurity firm and also from the Spanish National Police, which had attempted to contact it on three separate occasions. The institution did not take these warnings seriously because it believed they were attempts at fraud and it only activated its data breach protocol in October 2024, when its data protection officer accessed the forum and downloaded the sample.

In its decision, the AEPD concluded that the company had breached article 32 of the GDPR because it did not have in place security measures appropriate to the risk, even though it has not been possible to determine how the attacker gained access. The Agency highlighted two shortcomings: first, the systems were obsolete, and the company had known this since 2021 but did not replace them until January 2025, by which time the breach had already occurred; second, it did not have an effective incident management procedure in place. The Agency noted that the ability to detect a breach and provide a timely response is part of the security obligation itself and imposed a €30,000 fine.

A municipal council breaches the GDPR by disclosing to the press the reason for an identifiable employee's leave of absence

The AEPD has ruled that a local government entity breached article 5.1.f) of the GDPR, regarding the principle of integrity and confidentiality, by disclosing to a media outlet the specific reason why an employee was on leave of absence.

The case arose following the publication of a news item about operational difficulties in a municipal service. In this context, the public entity reported not only that the employee was on leave but also the specific reason for the leave. The AEPD considered that, although there was a legitimate interest in explaining the service's situation to the public, the disclosure of the specific reason for the leave of absence was not necessary to fulfill that information purpose. Moreover, the affected individual was easily identifiable because she held the only position of that nature within the organization.

The ruling underscored that administrative transparency does not justify the disclosure of personal data that are irrelevant for the intended purpose and reiterated that the principle of data minimization must be respected. The AEPD concluded that the disclosure constituted a breach of confidentiality regarding personal information and demonstrated a lack of adequate organizational measures to prevent such disclosures.

Due to the person at fault being a public authority, no monetary fine was imposed. However, a breach of article 5.1.f) of the GDPR as defined in article 83.5.a) of the same regulation was formally declared and the entity was ordered to adopt, within three months, technical and organizational measures designed to ensure the security and confidentiality of personal data in future public and institutional communications.

AEPD identifies information failures and insufficient impact assessment in biometric border controls

The AEPD has found that two breaches have taken place in relation to the border control

system used by a public agency responsible for border management. The case arose following a complaint from a passenger who reported being forced to undergo biometric screening at an airport without receiving adequate information about the processing of her personal data.

The decision confirmed that the use of biometric data to verify travelers' identities is legally permitted under European border control rules. However, the AEPD considered that the data controller breached article 21 of Organic Law 7/2021, of May 26, 2021, on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offenses or the enforcement of criminal penalties (applicable to the protection of personal data processed for the purposes of prevention, detection, investigation, and prosecution of criminal offenses and the enforcement of criminal penalties by the competent authorities), due to failing to provide data subjects with the required information regarding the processing of their data, their rights, the identity of the data controller, or the means of exercising those rights.

Furthermore, the AEPD concluded that article 35 of Organic Law 7/2021 had also been breached, by not having conducted a data protection impact assessment that fulfilled the legal requirements. The produced document did not adequately analyze the risks to the rights and freedoms of the data subjects, the life cycle of biometric data, or the measures envisaged to mitigate those risks.

Due to the person at fault being a public authority, no monetary fine was imposed. However, it determined that a very serious infringement of article 21 and a serious infringement of article 35 had been committed and ordered the adoption of corrective measures. These included providing effective information on data protection at border checkpoints and preparing an impact assessment that complies with legal requirements within three months.

AEPD concludes that a breach has taken place due to the failure to conduct an impact assessment in an AI-based virtual assistant project

The AEPD held that article 35 of the GDPR was breached due to the absence of a data protection impact assessment (DPIA) in the design of an AI-based virtual assistant project intended for citizen services.

The project involved the use of advanced technologies such as natural language processing, speech recognition, machine learning, emotional analysis and interaction via digital avatars. It also envisaged the collection of user identification data through a mobile app and the processing of interactions with the system to enhance its performance through continuous AI training processes.

The AEPD considered that these characteristics involved processing likely to pose a high risk to individuals' rights and freedoms, particularly due to the use of new technologies, the possibility of drawing inferences about users based on their interactions and the large-scale deployment of the system. It was therefore compulsory to conduct a DPIA before starting the project and during its design and procurement phases.

The supervisory authority rejected the argument that the system's failure to go live exempted it from this obligation. It noted that the impact assessment is a preventive measure that must be carried out from the earliest planning stages, when the characteristics of the processing are still being defined.

Due to the person at fault being a public authority, no monetary fine was imposed. The decision simply states that article 35 of the GDPR has been breached and dismisses the initial allegation regarding article 25 of the same regulation, after determining that the conduct was subsumed by the specific breach of the obligation to conduct the impact assessment.



Judgments

Right of access under article 15 of the GDPR does not generally extend to the identification of healthcare personnel who have accessed medical records

The judgment settles a cassation appeal that raised the question of whether the right of access recognized in article 15 of the GDPR includes the specific identification of healthcare personnel who have consulted a patient's medical record. The case stems from a complaint filed by a data subject who asked to know the identity of the personnel who had accessed their health data, a request that was denied by the AEPD and upheld in court.

In its judgment, Chamber Three of the Spanish Supreme Court concluded that the concept of "recipient" under article 15(1)(c) of the GDPR does not include employees or professionals who, as members of the data controller organization, access the information in the course of their duties and under the instructions of the controller. Therefore, the right of access does not generally include the identification of doctors, healthcare personnel, or authorized administrative staff who have consulted the medical record.

Relying expressly on case law by the Court of Justice of the European Union (Case C-579/21), the Supreme Court stated that the data subject could indeed obtain information regarding accesses made such as dates, purposes, or functional categories, in order to verify the lawfulness of the processing, but not the identity of employees who acted lawfully within the healthcare organization. It also stated that the identities of those professionals could only be disclosed in exceptional cases where such disclosure is necessary for the effective exercise of the rights recognized by the GDPR and after weighing those interests against the rights and freedoms of the employees concerned. It therefore dismissed the cassation appeal and confirmed that the AEPD's actions were in accordance with the law.

Court sets aside AEPD guidance on biometric attendance monitoring, holding that it has the substantive nature of a circular

The judgment settles an application for judicial review filed by the Spanish Association of Security Companies against the Guidelines on attendance control processing using biometric systems, published by the AEPD on November 23, 2023. The Chamber concluded in its judgment that the document could not be regarded simply as guidelines, but rather, in view of its substantive content, it effectively set out the Agency's enforcement and penalty criteria. In particular, the court emphasized that the guidelines established the criteria that the AEPD itself would apply in relation to attendance control using biometric systems and that those criteria were intended to produce effects on controllers and processors, which would have a substantial impact on the deployment and marketing of such technologies.

Applying the settled case law of the Spanish Supreme Court, according to which the legal nature of a provision depends on its substantive content and practical effects rather than on the name it receives, the Spanish National Appellate Court held that the guidelines constituted a circular in substance within the meaning of article 55 of Organic Law 3/2018 of December 5, 2018 on Data Protection and the Safeguard of Digital Rights (LOPDGDD). The guidelines should therefore have been drafted

in accordance with the specific procedure established for these types of regulatory instruments, including the relevant formal safeguards. As that procedure had not been followed, the Court declared the guidelines null and void and set aside their approval and publication. The judgment did not rule on whether biometric systems for time recording, attendance monitoring and access control are lawful and focused instead solely on the formal invalidity of the mechanism used by the AEPD to set out its interpretative criteria in this area.

Online publication of criminal judgments does not always qualify for the journalistic exception under the GDPR

In its judgment of July 9, 2026 handed down in case C-199/24 (*Legal Newsdesk Sweden*) by the Court of Justice of the European Union, the court examined whether the online dissemination, for a fee, of criminal convictions contained in a public database could benefit from the exceptions provided in article 85 of the GDPR in relation to processing carried out for journalistic purposes. The dispute arose after a Swedish platform refused to delete the personal data of a person convicted of a criminal offense that was contained in its database.

The Court noted that the member states should reconcile the right to the protection of personal data with freedom of expression and information but clarified that the exceptions envisaged in article 85.2 of the GDPR could only be applied to processing carried out for journalistic purposes and the purposes of academic, artistic or literary expression. As a result, the member states may not extend those exceptions to other activities through national legislation.

The CJEU also held that data subjects must retain the legal remedies recognized by the GDPR and therefore national legislation cannot limit protection to defamation action or claims for damages based exclusively on those grounds. The right to lodge complaints with the supervisory authorities and to bring legal action under the GDPR must remain fully guaranteed.

In relation to the definition of journalistic purposes, the Court adopted a broad interpretation, while requiring the existence of a genuine journalistic activity. Merely making criminal judgments available to the public for a fee, without any editing, adaptation, verification, or adherence to an editorial policy cannot automatically be regarded as a journalistic activity. The exception is only applicable where the dissemination of the information constitutes the genuine exercise of a journalistic activity carried out in accordance with editorial criteria and the ethical standards of the profession.

The ruling reinforces the protection of data relating to criminal convictions and limits the expansive use of the journalistic exceptions established in the GDPR for private databases that market judicial information accessible to the public.

CJEU rules that the GDPR precludes the indiscriminate publication of the personal data of all the shareholders of corporations

In its judgment of September 3, 2026 in case C-798/24 (Jautiva) the CJEU ruled on a request for a preliminary ruling referred by the Constitutional Court of Latvia regarding the compatibility with the GDPR of national legislation that required making available to the public, including the bulk downloading by unidentified users, the personal data of all the shareholders of corporations, including first and last names, personal identification numbers, contact addresses, email addresses, the class and number of shares and the number of votes attaching to those shares.

The Court concluded that article 14(d) of Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law, does not require the disclosure of information on all shareholders, including minority shareholders. It also reasoned that this provision refers to the appointment and removal of persons who, as a body or members of a body, represent the company in dealings with third parties or take part in its management, supervision, or control, and that shareholders are neither appointed nor removed, but rather that their status derives solely from their participation in the company's share capital.

Furthermore, the Court held that articles 5 and 6 of the GDPR, in light of articles 7 and 8 of the Charter of Fundamental Rights of the European

Union, must be interpreted as precluding national legislation which requires personal data relating to all the shareholders to be made available to the public without requiring proof of a legitimate interest. It also stated that the disclosure of minority shareholders' data is neither appropriate nor necessary, that the practical difficulties in verifying legitimate interest do not justify the interference and that the Latvian legislation did not have sufficient safeguards by allowing bulk downloading by unidentified users.

Loss of independence of the US Federal Trade Commission (FTC), following a U.S. Supreme Court ruling, weakens one of the pillars of the EU-US Data Privacy Framework

On June 29, 2026 the US Supreme Court delivered its judgment in Trump v. Slaughter. The judgment recognizes that the president may remove members of the Federal Trade Commission (FTC) at will. In doing so, it departs from a principle that had been in place since 1935, under which FTC commissioners could only be removed for specified causes. The decision ends the FTC's status as an independent agency and places it under the president's political control.

The FTC is the primary enforcement authority responsible for overseeing companies participating in the EU-US Data Privacy Framework (DPF). It investigates infringements, imposes penalties and ensures compliance with the privacy commitments undertaken by participating organizations. The European Commission expressly highlighted the FTC's independence in its July 2023 adequacy decision. That independence carries particular weight because EU law requires supervision in the field of data protection to be exercised by independent authorities:

- article 8(3) of the Charter of Fundamental Rights of the European Union;
- article 16 of the Treaty on the Functioning of the European Union;
- article 52 of the GDPR.

The two previous frameworks, Safe Harbor and Privacy Shield, were invalidated by the Court of Justice of the European Union (CJEU) in the Schrems I (2015) and Schrems II (2020) rulings. In both cases, the grounds were mass surveillance and the lack of effective remedies, not the FTC. This is compounded by the fact that the Privacy and Civil Liberties Oversight Board, the U.S. oversight body responsible for privacy and civil liberties matters, temporarily lost its quorum.

Organization *NOYB* has sent a letter to the European Commission requesting the orderly withdrawal of the Adequacy Decision. It has also announced a legal challenge that could lead to a *Schrems III*.

As of the date of this publication, the DPF remains fully in force and transfers to certified companies remain valid.

Supreme Court reinforces the duty to verify consent for advertising purposes where contracts are entered into through a representative

The Spanish Supreme Court has confirmed the penalty imposed on a company in the energy sector for failing to take adequate measures to verify that the persons acting as customer representatives were in fact authorized to consent to data processing for commercial and advertising purposes.

The case concerned the conclusion of energy supply contracts through various channels, which allowed representatives to act on behalf of customers, in many cases without requiring sufficient evidence of their authority to authorize additional processing of personal data. Such processing included sending commercial offers, receiving advertising for products and services unrelated to the contract and creating commercial profiles using information from third parties.

The AEPD found that articles 25 and 13 of the GDPR had been infringed and initially imposed fines of €500,000 and €1,000,000, respectively. The Spanish National Appellate Court subsequently reduced the fines to €250,000 for the infringement of article 25 and to €600,000 for the infringement of article 13, amounts that

were upheld following the cassation appeal that was filed.

The judgment clarifies that valid representation for the purpose of entering into a contract does not automatically imply that the representative is authorized to provide consent regarding data processing for purposes other than the performance of the contract. In such cases, the data controller must implement technical and organizational measures that enable it to evidence that the data subject has given free, specific, informed, and unambiguous consent, or that the representative has sufficient authorization to do so on the data subject's behalf.

CJEU holds that the GDPR does not preclude online publication of the names of professional athletes who have infringed anti-doping rules, but requires a prior balancing of the interests at issue

The case arose from the publication by the Austrian Anti-Doping Agency and the Austrian Anti-Doping Commission on their websites, of the names of athletes who had infringed anti-doping rules, together with the sports discipline practised, the infringement committed and the sanction imposed. Four athletes challenged the publication, arguing that the information disclosed fell within the concepts of data concerning health and personal data relating to criminal convictions and offenses, the processing of which is subject to enhanced safeguards under the GDPR. They further held that the undifferentiated publication system provided for in Austrian law was incompatible with the GDPR.

In the judgment handed down by the CJEU in case C-474/24, the court held that the GDPR does not, in principle, preclude the online publication of the name of the athlete, the sanction and the reasons, since it pursues an objective of general interest linked to combating doping, ensuring equal opportunities in sports and deterring anti-doping infringements. However, the Court imposed two conditions: first, the entity responsible for the publication must be able to balance the interests involved prior to the publication, observing the principle of proportionality, in particular as regards the length of time the data is retained on the website. Second, the athlete concerned must be able to lodge, as a preventive measure, a complaint with the data protection authority where that publication is imminent or will take place in the near future, which ensures effective protection before the dissemination of the data.

National Appellate Court overturns an AEPD penalty due to data processing in the management of an inheritance

The judgment concerns an application for judicial review filed by a financial institution against a decision of the Spanish Data Protection Agency that imposed a €100,000 fine for infringement of article 6(1) of the GDPR. The proceedings stemmed from the institution's opening of accounts in connection with the processing of an inheritance and the allocation of shares in an investment fund to minors, without having obtained the mother's express consent. The AEPD held that the processing lacked a legal basis, since the data provided to manage the inheritance could not be used to open those accounts.

The National Appellate Court disagreed with this assessment in its judgment and concluded that article 6 of the GDPR had not been infringed. The Court found that the data had been used in the administration of the inheritance requested by the heirs and that the opening of the accounts constituted a necessary step to carry out the operations inherent in the distribution of the estate and the allocation of the investment fund's shares. It also underscored that the accounts were in a preliminary stage, never became operational and required subsequent validation by the minors' legal representative. On this basis, it found that the processing was supported by a legal basis other than consent, since it was necessary for the performance of the steps required for the management and distribution of the inherited assets.

Consequently the court upheld the appeal, set aside the penalty imposed by the AEPD and ordered the refund of the amount paid by the financial institution together with the relevant statutory interest.

CJEU's Advocate General considers it insufficient to identify the recipients of data for commercial communications as partners

The CJEU has held the hearing in Case C-317/25, a request for a preliminary ruling referred by the French Council of State. The case stemmed from a €600,000 fine imposed by the French data protection authority (CNIL - *Commission nationale de l'informatique et des libertés)* on a French media group.

In 2021, the group sent electronic marketing messages to approximately 3.9 million people. The data came from two internet service providers. When signing up with these providers, users had ticked a box indicating their consent to the use of their data by the "partners" of those ISPs. The partners were not identified and there was no list available. The CNIL considered that such consent did not cover the marketing messages.

The Advocate General has delivered his Opinion in this case, in which a number of subscribers consented to their personal data being used for direct marketing purposes by the "partners" of two internet service providers (ISPs), without those recipients being specifically identified. Groupe Canal+ subsequently used those data to carry out electronic direct marketing campaigns and was fined by the French data protection authority.

According to the Advocate General's Opinion, consent can only be regarded as valid if it is freely given, specific, sufficiently informed and unambiguous. In order for the consent to be informed, the data subject must know the identity of the data controller that will effectively use the data. Therefore, the Advocate General takes the view that a generic reference to an ISP's "partners" does not mean that the data subject has consented to receive commercial communications from any company falling within that category.

Consequently, where the identity of the company intending to carry out the marketing was not known at the time consent was obtained, fresh consent must be obtained before using the data for that purpose, at the latest at the time of the first commercial communication. He also rejects the possibility that objecting or unsubscribing upon receipt of the first communication can remedy the absence of prior consent required by data protection regulations.

The Advocate General therefore concludes that a mere reference to an indeterminate category of recipients is insufficient to justify direct marketing activities. He nevertheless notes that his Opinion is not binding on the Court of Justice, which must rule on the matter subsequently by way of a judgment.

Advocate General proposes that the Court should find EU law incompatible with Belgian legislation on the retention of electronic communications data

The Advocate General delivered his Opinion in case C-661/24 in connection with a preliminary ruling requested by the Belgian Constitutional Court. He proposes that the Court of Justice should find that EU law precludes several provisions of the 2022 Belgian legislation relating to the collection and retention of identification data and traffic and location data in the electronic communications sector.

The Advocate General recalls that national measures requiring the retention of traffic and location data constitute an interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by the Charter of Fundamental Rights of the European Union. He states that such interference is permissible only if provided for by law, is strictly necessary and complies with the principle of proportionality.

In his analysis, the Advocate General acknowledges that, subject to certain strict technical conditions, the general and indiscriminate retention of data could be compatible with Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector provided that a genuinely watertight separation of the different categories of data is guaranteed, preventing their combined use and ensuring that precise conclusions on users' private lives cannot be drawn. However, he concludes that the Belgian legislation does not satisfy those conditions: it allows for the retention of

excessively broad categories of data, does not ensure a genuinely watertight separation, grants providers an excessive degree of discretion and fails to provide the guarantees of clarity, precision and proportionality required by EU law. The conclusions are not binding, and the Court of Justice will issue its judgment at a later date.

Contact our professionals

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

Sebastián Hassi
Senior associate - Santiago de Chile
sebastian.hassi@garrigues.com

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

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

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

Sebastián Barros
Partner· Santiago de Chile
sebastian.barros@garrigues.com

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

Antonio Durán
Associate - Málaga
antonio.duran@garrigues.com

Ignacio Suárez
Associate - Madrid
ignacio.suarez@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:

This publication is provided for information purposes only and does not constitute legal advice or advice of any other kind. It does not seek to offer a comprehensive summary of the legislation and developments to which it refers nor to cover all published material, but rather to provide an overview of selected topics. It is therefore recommended that the official texts be consulted and specific professional advice be sought. Garrigues does not accept any liability for the use made of this information and assumes no obligation to update it after publication.

© J&A Garrigues, S.L.P., all rights reserved. This work may not be used, reproduced, distributed, publicly communicated or altered, in whole or in part, without the written permission of J&A Garrigues, S.L.P.