GARRIGUES

Data Economy, Privacy and Cybersecurity Newsletter

November 2025

Contents

1. Is pseudonymized data personal data? Key points following the European Court of Justice's judgment in the *EDPS v SRB* case

The judgment delivered by the European Court of Justice (CJEU) on September 4, 2025 in the EDPS v SRB case (case C 413/23 P) is an important landmark in the field of data protection, because it deals with the concept of "personal data" which is at the heart of the practice.

Ignacio Suárez

The parties in this case were the European Data Protection Supervisor (EDPS) and the Single Resolution Board (SRB). The dispute stemmed from the resolution of Banco Popular (which took place under decisions by the SRB and the FROB in Spain on June 7, 2017) and the "right to be heard" procedure commenced by the SRB in 2018 to assess possible compensation for shareholders and creditors, in which data and comments were collected via an online register and form. The comments on "Valuation 3" (1,104 in total) were transmitted on June 17, 2019, by the SRB to Deloitte via a secure virtual server. Following several complaints, the EDPS found in 2020 that the SRB had not informed data subjects that Deloitte could be a recipient of this data in the confidentiality statement for the procedure, a decision (later revised) that the SRB challenged and which led to the CJEU judgment on September 4, 2025.

The most significant issue discussed in this case, which has generated intense and interesting debate among professionals in the sector, is whether pseudonymous or pseudonymized data is in itself personal data by default (because it is not completely and irrevocably anonymized), or whether it can be "non-personal" data for those who cannot, without disproportionate effort, link that data to an individual.

One might think that something so basic should not be up for debate at this stage, but the truth is that the wording of the legislation has given rise to different perspectives on what should or should not be considered personal data. This has resulted in the formation of two different viewpoints on this concept:

- **The absolute approach:** which treats as personal data any information that, directly or indirectly, could be associated with an individual, however remote or improbable this link may be.

- **The relative approach**: which treats that data as only personal for those who have reasonable means of linking this data to an individual.

It may be observed, therefore, under a strict application of the absolute approach it may be concluded that data is either personal or non-personal in itself, regardless of who has it in their possession. So, for example, a pseudonymized code would be personal data for a person, even if they were unable to link it to an individual, provided that somewhere, some controller had the "key" or correspondence table that would allow this re-identification.

This "monolithic" interpretation of the concept of personal data, while seeking to be particularly protective of the rights of data subjects, results in regulatory burdens that are sometimes unreasonable for data controllers. Despite this, it has long been the interpretation most often applied by the data protection supervisory authorities and, consequently, by operators, as it carries a lower risk of non-compliance for data controllers.

Recently, however, this interpretation has been refuted in CJEU judgments, such as in the *Breyer* and *Scania*. cases In these judgments, the court plumped for the relative approach, by finding, in short, that a dynamic IP address (in *Breyer*) or a vehicle identification number (VIN) (in *Scania*) are personal data only insofar as an entity can link that data to an individual.

Although it might be expected that, with the endorsement of those CJEU judgments, the relative approach has been fully instated and accepted, and this has diminished the importance of the judgment we are discussing, that is not the case. Certain authorities, such as the European Data Protection Board itself in its recent Guidelines 1/2025 on Pseudonymization - currently only available in a preliminary version for public consultation -, continue to adopt a decidedly restrictive approach, leaning more towards the absolute than the relative approach.

That is why the CJEU judgment discussed in this commentary is so significant, because beyond reaffirming the relative approach, it also states for the first time in crystal-clear terms that pseudonymized personal data (in this case, an alphanumeric code relating to a person) processed by controller "A" may be personal data for "A" and not be personal data for recipient "B" if the latter cannot (reasonably) link or re-identify the data.

Besides reaffirming the relative approach, this has important practical implications, as described below.

Practical implications

Since for controller "A" the pseudonymized data will, in any case, be personal data (because they have the ability to re-identify the data subject from the alphanumeric code), "A" must comply with the applicable legislation for all purposes. This means, among other obligations, that they must:

- have a legal basis (art. 6 GDPR) for processing that personal data, including, should the case arise, a sufficient legal basis for its disclosure to a third party; and provide information on the processing to the data subject, as required under articles 13 or 14 GDPR, as applicable, including information on the recipients of their personal data.

- The CJEU ruled along these lines in the discussed decision, although the details of the case show there is room for interpretation as to what type of information should be provided to data subjects on recipients who are not going to be able to establish the link between pseudonymized data and the data subjects.

Recipient B could be considered the controller for all purposes if it can reasonably reidentify the data subject. However, if, under the relative approach, recipient B is not considered the controller (because, from its point of view, personal data are not being processed), this poses difficult questions including:

What rights does the data subject have over the recipient of the data?

The judgment points out that the data subject can exercise its data protection rights against both the transferor and the recipient. For the latter, however, it might be materially impossible to respond, for example, to requests for access or erasure, because the information would not be personal for their purposes.

In that case, what information must the transferor provide to data subjects who are not able to identity the data subject?

In an attempt to rationalize the information requirements and avoid confusing scenarios between data subjects and the recipients who are unable to identity them, it could be considered that transferors: (i) should only provide information on the categories of recipients for whom the received information will not be personal information (without identifying each of the recipients individually); or (ii) should provide information to the effect that certain recipients will not be able to identity them with the received information, which will preempt the identified issues. As mentioned above, on this point the CJEU's decision leaves some room for interpretation (in view, for example, of the legal basis they apply in each case).

Does this apply to data processors?

In relation to data processor relationships, significant doubts arise as to whether this approach applies where the "processor" operates on the instructions of the controller but processes pseudonymous data which does not constitute personal information for the processor. Prudence suggests that the relative approach would not be fully applicable. This is because if the processor is operating on behalf of the controller, it is difficult to argue that the processor is processing "non-personal" data (as it is following the controller's instructions, the likelihood of re-identification should not be considered remote in any case). However, this case needs to be studied further, because the practical implications of accepting that the relative approach is fully applicable for these purposes would be huge (consider the benefits it would imply for contracts with third parties).

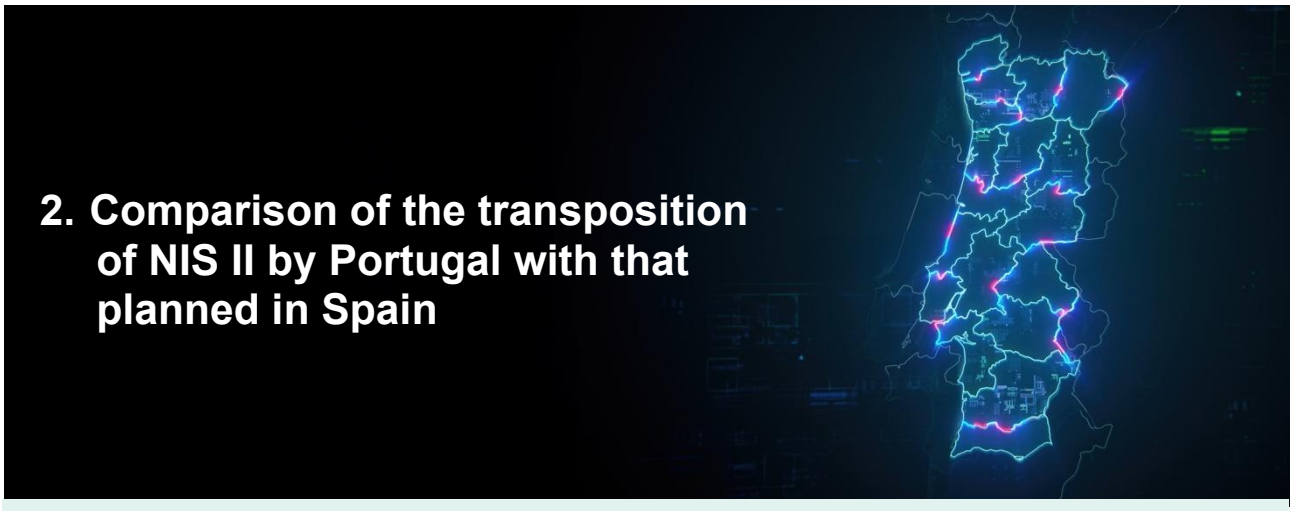
Conclusion

The CJEU ruling in the *EDPS v SRB* case not only reaffirms the known relative approach, it also provides a major milestone to guide practitioners by giving highly relevant insights into implementation of this approach. In particular:

- It clarifies that pseudonymous data may or may not be personal data, depending on who processes it and the actual chances of identifying individuals, and provides guidance on the obligations of transferors and recipients of pseudonymized data, which must be studied in detail for their correct adoption.

- It opens up new ground to be explored by data protection professionals, who will have to take its conclusions into account when structuring compliance systems for controllers and processors. For example, its implications on the use of pseudonymized information for AI model training may be of great interest to holders of large volumes of personal information, as it could facilitate its sale.

- This judgment requires a new perspective not only with regard to new transfers or data processing engagements to brought into compliance, but also a rethinking of the structures already in place, which could be affected by this interpretation of the legislation.



2. Comparison of the transposition of NIS II by Portugal with that planned in Spain

In July 2025, the Portuguese government resumed the process of transposing Directive (EU) 2022/2555 (NIS2) by presenting Bill no 7/XVII/1 Below we compare this transposition with the Spanish bill, examining the areas of application that are subject and exempt in each case, as well as the planned penalty system.

Manuel Liberal Jerónimo and Luisa Cyrne

Portugal's previous bill (Bill no 50/XVI/1) expired with the dissolution of the Assembly of the Republic on March 11. Portugal currently remains in breach of the October 2024 transposition deadline, which led to the European Commission opening infringement proceedings in November that year.

Compared with the Spanish bill (Preliminary Bill for the Law on Coordination and Governance of Cybersecurity), one of the main differences relates to the scope of application:

Scope of application

Portugal	Spain
Private entities	**Public or private entities**
▪ **From critical sectors:** Energy; transport; banking; financial market infrastructure; health; water; digital infrastructure[1]; managed service providers; and space. ▪ **From other critical sectors:**	

[1] This includes providers of internet exchange points, DNS services, TLD name registries, cloud computing services, data center services, content delivery networks, trust services, public electronic communications networks, and publicly available electronic communications services.

Portugal	Spain
Postal and courier services; waste management; production, manufacturing, and distribution of chemicals; production, manufacturing, and distribution of food products; manufacturing; provision of digital services[2]; research. **Spain also adds: the nuclear industry and private security sectors.**	
■ Public authorities ■ Office of the Ombudsman. ■ Economic and Social Council. ■ Technical and administrative services of the Presidency of the Republic, the Assembly of the Republic, the Courts, the Superior Council of the Judiciary, the Superior Council of Administrative and Tax Courts, and the Superior Council of the Public Prosecutor's Office.	■ Government administration entities, excluding the judiciary, parliaments, and central banks.
■ Higher education institutions.	■ Universities and research centers (for matters or research projects related to critical sectors)
Critical entities (to be designated).	

Excluded from the scope of application

Portugal	Spain
■ General Staff of the Armed Forces and branches of the Armed Forces[3]. ■ Public entities with criminal investigation responsibilities and criminal police and public security forces. ■ Public entities with exclusive responsibilities in the production of information, namely the Intelligence System of the Portuguese Republic, the Strategic Defense Intelligence Service, and the Security Intelligence Service.	■ Government administration entities carrying out activities in the fields of national security, national defense, or public safety, including the prevention, investigation, detection, and prosecution of criminal offenses, except for activities in which they act as trusted service providers available to third parties. ■ Instituto de Crédito Oficial (Official Credit Institute)

[2] This includes providers of online marketplace services, online search engine services, and social media platform services.

[3] In relation to networks and information systems directly related to their command and control.

Portugal	Spain
■ Public entities whose activity focuses on information networks and systems directly related to the production and dissemination of classified information, specifically with national markings, from the North Atlantic Treaty Organization (NATO) and the European Union, or classified as state secrets, in relation to these information networks and systems. ■ Other public entities that carry out their activities in the fields of national security, public security, defense, and intelligence services, with regard to networks and information systems directly related to the activities relating to the production of information and the prevention, investigation, detection, and prosecution of criminal offenses. ■ Private entities providing services exclusively to one or more of the entities referred to in the preceding paragraphs and in relation to these activities.	

Both proposals adopt the same methodology and criteria for classifying entities covered as **essential** entities. The classification of entities as **important** entities also adopts the same classification criteria, and Spain also includes municipalities with more than 20,000 inhabitants and entities in its institutional public sector. Portugal has chosen to include an article dedicated exclusively to public entities that are not classified as essential or important entities, and classifies them as relevant public entities along with dividing them into two groups for the purposes of applying specific regimes as determined in the proposal and other regulations issued by the National Cybersecurity Center.

Some differences in the penalty regime may also be expected:

Penalty regime

Administrative infringement	Portugal	Spain
Very serious	Committed by an essential entity: ■ Between €2,000.00 and €10,000,000.00 or up to 2% of their gross worldwide annual revenue, in the previous fiscal year. ■ Between €350.00 and €200,000.00, if carried out by an individual. Committed by an important entity:	Total: between €500,001.00 and €2,000,000.00. Committed by an essential entity: the fine can amount to €10,000,000.00 or 2% of the previous year's gross

Administrative infringement	Portugal	Spain
	■ Between €1,250.00 and €7,000,000.00 or a maximum amount of no less than 1.4% of gross worldwide annual revenue. ■ Between €350.00 and €200,000.00, if committed by an individual. Committed by a relevant public entity (depending on whether it belongs to group A or B): Between €8,000.00 and €4,000,000.00.	worldwide annual revenue. Committed by an important entity: the fine can amount to €7,000,000.00 or a maximum amount of not less than 1.4% of gross worldwide annual revenue.
Serious	Committed by an essential entity: ■ Between €1,250.00 and €5,000,000.00 or 1% of the previous year's gross worldwide annual revenue; ■ Between €250.00 and €125,000.00, if committed by an individual. Committed by an important entity: ■ Between €875.00 and €3,500,000.00 or a maximum amount of not less than 0.7% of gross worldwide annual revenue; ■ Between €250.00 and €125,000.00, if carried out by an individual. Committed by a relevant public entity (depending on whether it belongs to group A or B): Between €5,000.00 and €225,000.00.	Total: between €100,001.00 and €500,000.00.
Minor	Between €875.00 and €45,000.00, if committed by a legal entity. Between €250.00 and €3,750.00, if committed by an individual.	Total: between €10,000.00 and €100,000.00.

Broadly speaking, the proposals are quite similar in terms of the obligations envisaged for entities falling within their scope, and both proposals reflect a clear commitment to improving cyber resilience, with featured elements and nuances that underscore the priorities and institutional models of each member state.

3. Data protection authorities' decisions

Local council fined for sending proof of payment of a fine to an outdated address

The AEPD decided on an enforcement proceeding against a local council for sending proof of payment of a traffic fine to the complainant's outdated address, where her ex partner lives.

The document contained the complainant's personal data, including her vehicle registration number, date, and place of the infringement. The complainant had updated her address with the traffic authority (DGT) and had notified the local council's enforcement agent, but the receipt was sent to an old address that had been in the fines database since 2013. The local council argued that the receipt was not part of the enforcement proceeding and that the system automatically selected the address because the information had not been updated before payment.

The AEPD held that the local council had violated the principles of integrity and confidentiality (art. 5.1.f GDPR) and accuracy (art. 5.1.d GDPR), by not applying the appropriate technical and organizational measures to ensure the security and updating of the personal data. The decision highlights that the complaint form delivered by hand, on which the individual concerned expressly provided her current address, was not taken into account by the computer system when generating the payment receipt. The receipt was automatically sent to an old address recorded in the fines database, and an updated request had not been made to the DGT.

If was held, therefore, that there had been a very serious breach under article 83.5.a GDPR and article 72.1.a of the Spanish data protection law (LOPDGDD), and notification of the Ombudsman was ordered.

Dismissal of appeal by a telecommunications company against a penalty for fraudulent duplication of SIM cards

The AEPD dismissed an appeal lodged by a telecommunications company against an enforcement decision dated November 8, 2024 imposing a €200,000 fine for a breach of article 6.1 GDPR.

The penalty arose following the fraudulent issuing of a duplicate SIM card to a third party, without a valid legal basis or the cardholder's consent. The company claimed it had followed its internal protocols and acted with due diligence, but the AEPD concluded that these measures were insufficient to ensure the lawfulness of the processing. The agency emphasized that responsibility for the processing lies with the operator, who must adequately verify the identity of the applicant and ensure that the processing complies with the GDPR. The mitigating circumstances

relied on by the fined entity, such as cooperation with the AEPD, absence of any benefits, and non-inclusion of sensitive data, were rejected because they failed to meet the requirements. In addition, the recurrence of similar breaches and the direct link between the business activity and the processing of personal data were considered aggravating factors.

The decision emphasizes that issuing a SIM card to a third party without authorization constitutes unlawful processing, with the potential to enable serious fraud such as access to bank accounts or social media. The AEPD reaffirmed the need for deterrent and effective penalties and pointed out that in addition to having measures in place, proactive responsibility also requires ensuring their effectiveness at all times.

Chain of shopping malls fined for several personal data breaches and security measures

The AEPD has imposed three fines on a shopping mall chain amounting in total to €3,200,000 for breaches of the GDPR.

The decision stemmed from five security breaches reported between January and September 2023, affecting 118,895 individuals in total. The attacks used credential stuffing techniques to enable unauthorized access to personal data such as name, address, email, date of birth, and login credentials. The AEPD concluded that the entity breached article 5.1.f) GDPR (principle of integrity and confidentiality), article 32 (security of processing), and article 34 (communication of breaches to data subjects).

The company submitted that it had adapted technical and organizational measures, such as audits and two-factor authentication, but the AEPD considered that they were late, insufficient, or had not been adequately implemented. It was also found that the communications sent to data subjects were not compliant with the requirements under article 34 GDPR, because they omitted essential information about the nature of the breach and the adopted measures.

The AEPD considered to be aggravating factors the scale of the compromised data, negligence in the management of security, and a direct link between the company's business activity and the mass processing of personal data.

Fine imposed on gas and electricity company for fraudulent agreements for services

The AEPD has fined a gas and electricity company €100,000 for contravening article 6.1 GDPR, by engaging in an illegal processing of personal data without any legal basis.

The complaint was filed by an individual who reported that he had been signed up for gas, electricity, and related services without his consent. The fined entity claimed that the contracts were managed by a partner company, acting as data processor, and that this company acted fraudulently and outside its instructions.

The AEPD concluded however that the company did not conduct adequate monitoring of its processor, thereby breaching its duty of supervision and allowing the processing of data without any legal basis. Although the contracts and invoices were canceled following the complaint, the agency considered that the company did not prove that it acted with the required diligence. The decision emphasizes that the controller can be penalized for the actions of its processors where compliance with the GDPR is not ensured.

The breach was classified as very serious, under article 72.1.b) LOPDGDD. The AEPD considered to be aggravating factors the nature of the processing, the volume of data concerned, and the link between the business activity and the mass processing of personal data.

Electricity retail company fined €200,000 for entering a customer on an overdue payments file before notification of the request for payment was returned

The AEPD has imposed a €200,000 fine on an electricity retail company for entering a customer's data on a file without meeting the requirements under article 20.1 LOPDGDD, which amounts to a processing of data without any legal basis under article 6.1 GDPR.

The complainant submitted that he had not received a payment request or any information about possible inclusion in overdue payments systems. Although the respondent produced a payment request, it was returned by the postal service on a later date than the entry in the overdue payments file, which evidences that it was made without confirming the receipt or return of the request. Therefore, the AEPD concluded that the obligation to inform the data subject in advance, as required by article 20.1.c), which stipulates that the data subject must be forewarned in the contract or at the time of the payment request, was not fulfilled.

The penalty was increased on account of the nature of the breach which has an effect on the claimant's credit record, the link between the defendant's activity and the processing of personal data, and the negligence shown by including the data without the debt meeting the legal requirements.

Telecommunications company in Germany fined for supervision and security failures

The Federal Data Protection Authority in Germany has imposed two administrative fines on a telecommunications company totaling €45 million, in addition to issuing a warning, due to serious deficiencies in the supervision of data processors and in the security of its online services portal.

The respondent, which operates through in-person stores managed by partner agencies acting as data processors, had data processing agreements, although they were not appropriately supervised and audited. This led to vulnerabilities in the IT systems which facilitated the misuse of personal data in cases of fraud. As a result, a €15 million fine was imposed and a warning was issued for insufficient supervision and technical weaknesses.

On top of this, the entity was fined a further €30 million for failures in the authentication mechanisms for its online portal, which, combined with telephone support, enabled misuse of eSIMs.

AEPD concludes that the right to data portability does not apply in a state education context, but upholds a complaint for untimely response

The complainant filed a complaint against the Regional Ministry of Education of the Junta de Castilla y León, arguing that their right to the portability of their daughters' personal data, as students at different state schools, had been neglected, because they had not received any response from these schools within the one-month period set by the regulation. The data related in particular to the psycho-educational assessments of their daughters in the period between 2018 and 2023.

The complainant submitted that the regional ministry's educational institutions have electronic platforms that allow data to be sent directly from one controller to another, and therefore the regional ministry can make those documents available via the electronic notification system. The respondent stated that the requested documentation is available to the complainant at the respective schools, because health data cannot be sent to private email addresses, which applies to the address of the private psychology facility from which the portability was requested.

In its decision, the AEPD took the view that, due to being an administrative and non-contractual relationship (between a state school and parents), governed therefore by state education legislation, the right to data

portability does not apply to this case, based on recital 68 and article 20 GDPR.

i. Recital 68 GDPR states that "that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller."

ii. Article 20 GDPR: "That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

The AEPD concluded that the right to portability does not apply in this case, but it upheld the complaint on procedural grounds because the response was issued late, although it acknowledged that no further action was required on the part of the respondent.

Employee fined €300 for a breach consisting of processing personal data without any legal basis

Initially, an individual filed a complaint against a company engaged in the retail sale of fruit and vegetables because she had been contacted by a company employee in personal WhatsApp messages. The complainant believed that the employee had obtained her data from the information she had provided for management of the "Salamanca Tarjeta Activa" card, used to obtain discounts at local shops.

In the right to be heard procedure, the respondent stated that it had obtained the data directly from the complainant, and submitted that she was a repeat customer who placed express orders for which she had to be contacted, and that the complainant actively participated in a Christmas raffle for which her data had to be left. However, although the complaint was initially rejected, the complainant appealed, categorically denying the allegations made by the other party, highlighting the personal nature of the messages sent and referring to the lack of evidence to support the claims made by the defendant.

The AEPD decided to uphold the appeal and order continuation of the proceeding to carry out investigative actions to determine the person responsible for the processing and its origin. It was found that the person who communicated with the claimant was indeed an employee of the company, who did so from a personal mobile phone and that, in addition, the origin of the data was, as submitted by the complainant, a transfer of data from the platform managing the "Salamanca Tarjeta Activa" card for partner businesses, including the entity against which the compliant was brought.

The AEPD therefore decided to initiate disciplinary proceedings and, in light of the facts, concluded that the employee used the personal data that the complainant had provided to the respondent entity for professional reasons, not to its employee for personal reasons. Consequently, it was inferred that the employee acted on his own behalf and not on behalf of or on instructions given by his employer, so the processing transactions carried out were not covered by contractual lawfulness which was a basis available to the entity. Lastly, the AEPD imposed a €300 fine on the employee for a breach of article 6.1 GDPR, as defined in article 83.5.a) GDPR.

AEPD dismisses complaint regarding the installation of a digital peephole viewer, and does not find a data protection breach

On June 19, 2025, the AEPD decided on a proceeding stemming from a complaint filed by a neighbor in a homeowners' association against another neighbor, alleging that the latter had installed a digital peephole on his door without prior authorization from the

homeowners' association. He also stated that the device was able to record images of communal areas and was not properly marked.

The AEPD ordered dismissal of the proceedings under general criteria in relation to digital peepholes: (i) they are allowed if they perform a similar function to a conventional peephole; (ii) it is not necessary to apply to the homeowners' association to install one; (iii) the area they cover (landings) is not part of the private sphere of individuals, as they are simply transit areas; and (iv) as a general rule, digital peepholes do not store data so it is not necessary to place a sign informing of their existence. Added to this, the evidence produced was insufficient to rebut the presumption of innocence to which the respondent was entitled.

Finnish pharmaceutical company fined €1.1 million for deficiencies in the protection of data at its online store

The fined pharmaceutical company used cookies and other tracking technologies at its online pharmacy, which transmitted user data packages directly to companies such as Meta and Google, including user interactions with different prescription and over-the-counter medicines, as well as IP addresses and other data from which users could be identified.

If a user was connected to their Google or Facebook account when they used the online pharmacy, Google and Meta could have identified them directly. This is particularly significant in view of the sensitive nature of the data, because it relates to people's health.

The Finnish authority therefore held that the company had breached articles 5, 25 and 32 GDPR due to the absence of appropriate technical and organizational measures, and imposed on the pharmaceutical company an administrative penalty consisting of a €1.1 million fine.

Private party fined for installing cameras positioned towards a neighbor's dwelling

The AEPD has fined a private party for installing video surveillance cameras positioned towards the main entrance and swimming pool of an adjacent dwelling. The complaint dates back more than four years, when the affected party reported to the AEPD that the presence of the cameras was an invasion of their privacy. In 2019, the complainant unsuccessfully attempted mediation through the local council. Subsequently, the AEPD attempted to send a request to the respondent to report on the measures taken, but the notice was not served due to delivery incidents. Finally, in September 2024, disciplinary proceedings were initiated.

The respondent claimed that the cameras installed outside his home did not record or provide video surveillance, and that their only purpose was to deter theft or vandalism. A visual inspection by the police confirmed that the cameras were not working.

In its decision, however, the AEPD warned that the simply fact of being able to capture images of other people's spaces, even it they are not recorded, constitutes a processing of personal data, and it held that these circumstances affect the privacy of the individuals concerned, creates a perception of surveillance and entails a disproportionate measure due to not being restricted to protection of a person's own property. Consequently, the AEPD concluded that article 5.1.c GDPR had been breached, and imposed a €500 fine.

Logistics company fined €100.000 for requesting a criminal record certificate and excessive personal data in recruitment processes

The AEPD has fined a company engaged in logistics, storage, and transport of goods €100,000 for requesting unnecessary information from candidates in recruitment processes. A complainant reported that, to be able to have a job interview, he was asked to

submit a criminal record certificate and fill out a form asking for his marital status and number of children.

The company claimed that the request for the certificate was justified under Implementing Regulation (EU) 2015/1998, which requires criminal record checks for staff with access to air cargo areas, and that the marital status and number of children data were requested in order to complete form 145 of the Spanish Tax Agency, relating to the communication of data on the recipient of employment income. In its decision, however, the AEPD held that European law only authorizes a criminal record check on the individuals who are ultimately recruited, not on every candidate in the interview process, and so the practice of requesting this certificate entails an unjustified mass processing of data on criminal convictions. Lastly, the agency clarified that the data requested for form 145 must only be collected after the employment relationship has been formalized, not during the recruitment process.

For all these reasons, the AEPD concluded that the company had breached article 5.1.c) GDPR (relating to the principle of data minimization), as well as article 10 of the same regulation and article 10 LOPDGDD, in relation to the processing of data on criminal convictions. And therefore it handed out two fines: €75,000 for the unjustified request for a criminal record certificate and €25,000 for the collection of personal data before it is necessary

Entity fined €32,000 for disclosing a worker's medical data to a third party

The AEPD has fined an occupational risk prevention entity €40,000 (reduced to €32,000 for voluntary payment) for violating the principle of confidentiality in the processing of personal data, under article 5.1.f) GDPR.

The proceedings were initiated following a complaint from an employee who discovered when accessing his medical report on the prevention service's web platform that the document included medical tests belonging to another employee. The incident was caused by an error in the document scanning and uploading process, which enabled unauthorized access to particularly sensitive information.

The AEPD considered that the entity did not apply adequate organizational measures to prevent a situation of this type, which led to a loss of control over personal data by the data subject. Although the company claimed that it was human error and submitted corrective measures such as staff training, protocol reviews, and security certifications, the agency concluded that these actions were taken after the fact and did not exempt it from liability.

The breach was classified as very serious, because it affected health data, which is classed as specially protected under the legislation. Although a potential breach of article 32 GDPR (security of processing) was assessed initially, it was rejected because the absence of general technical measures had not been proven.

Entity fined €180.000 for breaching a final decision by the AEPD

The AEPD fined an entity €225,000 (reduced to €180,000 for voluntary payment) for failing to comply with a final decision ordering it to comply with the right of access exercised by a data subject under article 15 GDPR.

The proceeding was initiated after the entity repeatedly refused to respond to the AEPD's requests, calling on it to provide the complainant with a certificate of access or a reasoned refusal in ten working days. Despite multiple requests between March and October 2024, the company failed to prove that it had complied with the decision, and consequently the AEPD initiated an enforcement proceeding for a breach of article 58.2 GDPR, which requires compliance with the orders of the supervisory authority.

The entity pleaded confusion with similar proceedings and the absence of any intention to breach the law, but the AEPD rejected these reasons, and pointed out that compliance with

final decisions is enforceable regardless of internal errors. The AEPD also classified the breach as very serious under article 72.1.m) LOPDGDD, and highlighted the importance of the principle of proactive responsibility, which requires the controller to ensure and evidence compliance with the GDPR throughout the data processing cycle.

The penalty was graded by reference to factors such as the duration of the breach (over more than a year), the repeated requests and fact that it affected one data subject. Lastly, the entity elected voluntary payment, which gave rise to early termination of the proceeding.

AEPD endorses storage of personal data by a processor after the end of the engagement

In this case, a processor objected to deleting the personal data falling under a data processing agreement after the contractual relationship with the controller had ended. Instead, the processor stored the blocked data, arguing that this was necessary to ensure it could exercise the right to defend its legitimate interests, because it was involved in a dispute with the controller.

In its decision, the AEPD held that a provision in article 33.4 LOPDGDD allows this step by stating that: "The processor may store the data, duly blocked, insofar as liabilities may arise from its relationship with the controller." Therefore, by combining this provision with the right to effective judicial protection, the AEPD dismissed the case.

Although the AEPD did not explain in detail any of the interesting concepts arising in the decision -such as blocking - or specify in detail the regulatory implications of the storage of this data by the processor outside the framework of the data processing agreement (by referring, for example, to its role at that time, the duty to inform data subjects, the legal bases at stake in this context, etc.), this is a decision to be taken into account, because it highlights a very common issue in practice, which is not often discussed in the sector, namely the authorization under article 33.4 LOPDGDD.

AEPD finds that, to comply with article 28 GDPR, it is not sufficient to mention in the DPA that the data will be deleted or returned when the processing has ended

In relation to a penalty arising from a security breach experienced by the processor providing services to the controller, the AEPD held to be insufficient the general clause usually included in data processing agreements in which the processor undertakes to delete or return the data after the service ends.

The AEPD held in this respect that the controller must, if not expressly stated in the contract, issue clear and operational instructions to ensure that the processor complies with the same storage periods as apply to the controller, so that the processor does not store all the data until the end of the agreement where it is no longer necessary.

The decision imposes a €250,000 fine on the controller for breach of article 5.1.f GDPR and another €50,000 fine for breach of article 28 GDPR.

French supervisory authority fines Google and Shein for installing cookies and similar technology without consent

The French data protection authority (CNIL) has imposed record fines: €325 million on Google and €150 million on Shein, under its action plan on cookies and digital advertising.

In relation to Google, the authority identified that the company inserted email-format advertisements in the "Promotions" and "Social" tabs in Gmail without obtaining users' prior consent, which constitutes electronic prospecting prohibited by French law. Moreover, the process for creating accounts with Google did not ensure valid consent for the installation of advertising cookies, as the

information was insufficient and the refusal option was difficult to find.

Whereas Shein was fined for installing advertising cookies on users' devices before they could express their consent, and for using incomplete information banners that did not adequately explain the advertising purposes or identify the third parties involved. The CNIL also found that, even after users rejected cookies or withdrew consent, trackers continued to be installed and read.

Both decisions underscore the importance of obtaining prior, free, and informed consent before any data processing for advertising purposes, as well as offering rejection mechanisms that are equally accessible as those for acceptance. The CNIL warned that it will continue to actively monitor compliance, especially with regard to misleading or disproportionate practices in the design of banners and flows to obtain consent from data subjects.

AEPD does not endorse use of employee photographs for working time monitoring

The AEPD examined the lawfulness of a working time monitoring system implemented by RENFE INGENIERÍA Y MANTENIMIENTO SME, S.A., which combines the use of an ID card combined with a photograph taken when workers clock in, and is different for central offices (card only) and maintenance bases (card and photograph).

Under article 4 GDPR, a photograph is personal data, but is not biometric data, because specific technical measures are not used for automatic identification, instead verification is carried out manually by HR. Compliance with the principles under article 5 GDPR was examined, especially in relation to lawfulness, minimization, purpose limitation, and security, as well as the legal basis for recording working hours, which is compliance with a legal obligation, fraud prevention, and management of the contractual relationship by monitoring working activity (articles 20.3 and 34.9 of the Workers' Statute).

It was proven that the information given to workers is adequate, that the processing is necessary and proportionate, and more intrusive alternative methods were cast aside. Therefore, no breach was found, because the system does not violate the principles under the GDPR nor does it involve the processing of biometric data. The proceedings were dismissed.

Football club fined for security breach caused by ransomware attack

The AEPD fined a football club for a security breach caused by a ransomware attack involving the personal data of approximately 60,000 people, including specially protected data.

The AEPD based its jurisdiction on article 58.2 GDPR and the LOPDGDD, and pointed out that as controller the entity must ensure the integrity and confidentiality of the data (art. 5.1.f GDPR), and apply technical and organizational measures appropriate to the risk (article 32 GDPR).

The decision notes the absence of sufficient measures, such as network segmentation and data encryption, which allowed the attack to compromise all the virtualized servers and backups. It highlights the seriousness of the breach due to the volume and sensitivity of the data concerned, as well as the duration of the breach.

The conduct was classified as a very serious (art. 83.5 GDPR and art. 72 LOPDGDD) and a serious breach (art. 83.4 GDPR and art. 73 LOPDGDD), and a €110,000 total fine was imposed, which was reduced to €66,000 due to acknowledgment of responsibility and voluntary payment. It also ordered the adoption of corrective measures to bring the security into line with the GDPR.

AEPD fines technology company for transfer of personal data to third parties without having sufficient legal basis

The complainant, an association that promotes democracy and digital rights, filed a complaint with the AEPD against a technology company, alleging that the personal data of self-employed workers provided to AEAT and to the Commercial Registry for registration on the list of individuals and businesses engaged in economic activities was subsequently processed and transferred to third parties - including the Chamber of Commerce, Camerdata, and private consulting firms - for commercial and marketing purposes, without sufficient legal basis and without sufficient information being provided to the data subjects. The complaint emphasized that this data, which included identifiers such as tax identification numbers, was accessible online and was used for purposes other than those initially reported.

During the investigation, the AEPD gathered information from the entities involved. The reported entity defended the lawfulness of the processing by invoking legitimate interest, the public source origin of the data, and the adoption of indirect information measures. The AEPD concluded, however, that the processing fell outside the legal framework in Law 4/2014 on Chambers, due to being intended for the mass marketing of databases for marketing campaigns, and that the presumption of lawfulness in article 19 LOPDGDD did not cover the use of identifying data such as taxpayer identification numbers. It also found a breach of the duty to provide information under article 14 GDPR, because it was not ensured that data subjects were effectively informed.

Consequently, the AEPD upheld the complaint, held that articles 6.1 and 14 GDPR had been breached, imposed €24,000 and €18,000 fines respectively, and ordered cessation of the processing and deletion of data processed without any legitimate basis.

Travel company fined for violating data minimization principle

The decision stemmed from a complaint brought with the AEPD against a travel company on the ground that the entity had unlawfully requested complete copies of guests' identity cards during the online check-in process to book accommodation, which involved, in the complainant's opinion, an excessive request for personal data.

The complainant alleged that, although he had provided the required identification data, the respondent insisted on the need to send a complete copy of his identity card, claiming that it was essential to comply with the legal obligations relating to registration and communication to the police forces. The respondent alleged that it requested complete pictures of guests' identity cards as part of the identity verification process, under Royal Decree 933/2021, and provided justification that in-person verification was not feasible in its digital business model.

However, after analyzing the applicable legislation and the principle of data minimization in the GDPR, the AEPD held that the request for a complete copy of the identity card exceeded the data strictly necessary for the intended purpose, since the legislation only requires the collection of certain identifying data rather than a complete copy of the document. The AEPD consequently upheld the complaint, held that the respondent had violated the data minimization principle under article 5.1.c) GDPR, and imposed an administrative fine amounting to €70.000, which was acknowledged and paid voluntarily by the respondent, and therefore reduced to €42,000. It also ordered corrective measures to bring its procedures into line, by removing the requirement to produce a copy of the guest's identity card and deleting all previously collected pictures.

Polish Data Protection Authority imposes separate fines on controller and processor for negligence in risk analysis and in adoption of security measures

The Polish Data Protection Authority has fined a restaurant chain €4,022,773 and one of its data processors €43,680, after finding serious deficiencies in risk analysis and in the

adoption of security measures in the processing of personal data.

The case originated from the notification of a security breach that exposed sensitive data of employees and franchisees in a file that was accessible to the public. The investigation revealed that neither the controller nor the processor carried out an adequate risk analysis or implemented technical and organizational measures proportionate to the nature and scale of the processing, thereby breaching articles 24, 25, 28, 32, and 38 GDPR. Additionally, the processor subcontracted services without the required sub-processor agreement, and the data protection officer was not appropriately involved in security management, which limited the organization's preventive capacity.

The decision highlights the importance of effective supervision, continuous updating of security measures, and the active involvement of the data protection officer in all processes related to data protection.

4. Judgments

The National Appellate Court upholds a penalty imposed by the AEPD for processing without a legitimate basis due to the publication of lists with the names and surnames of civil service candidates

The National Appellate Court confirmed the €12,000 fine imposed on a company by the AEPD in August 2022 due to publishing on its website, lists of the results of a selection process held in the context of a competitive examination organized by the Health Service of Galicia (SERGAS), which contained the names and surnames of the candidates without their consent.

The conflict arose because the entity in question had modified the provisional score lists of the selection process for the Administrative Officials Auxiliary Group of the SERGAS, which had initially been officially published by this entity in 2019. While the original lists were arranged in alphabetical order and mixed up different shifts, the fined entity had reorganized the data by scores and classified them into three categories: "Open Access", "General Disability" and "Internal Promotion". These lists included the names and surnames of the applicants, which, according to the AEPD, constituted undue processing of personal data, since it did not comply with the legitimate purposes of the original publication.

The judgment rejected the company's arguments regarding anonymization, legitimate interest, and the proportionality of the penalty and concluded that its actions were not covered by the legislation, as they constituted additional data processing without an adequate legal basis. According to the judgment, altering the original format of the personal data and classifying it by score, rather than following the officially established alphabetical order, altered the original purpose of the processing which breached the principles of the GDPR. In particular, the Chamber underscored that the data subjects had not given their express consent and that there was no other valid legal basis to legitimize this reconfiguration of personal data.

Consequently, the judgment dismissed the appeal for judicial review filed by the entity that had received the penalty and confirmed the AEPD's decision in full, which had imposed the €12,000 penalty.

Galicia High Court examines use of algorithms in selection processes and confirms labor union discrimination by a port authority

This judgment by the Galicia High Court was in connection with an appeal filed by a port authority against a ruling by a labor court in relation to a claim brought by an individual on the grounds of a

breach of fundamental rights. Specifically, the debate hinged on whether the entity had breached the fundamental right of freedom of association in processes related to functional mobility and access to certain jobs in the organization, in connection with the use of predictive algorithms.

In 2017, the port authority applied functional mobility criteria to temporarily fill various jobs, using a system of profiles and technical scales to select candidates, taking into account factors such as the technical distance from the ideal profile for the position.

The complainant alleged union discrimination during these processes, since, although she had been listed on several occasions as the most suitable candidate according to the objective evaluation criteria, the company chose to select other workers. According to the plaintiff, the decisions were dismissed or altered by subjectively considering other factors, such as the influence of union positions, pointing out that her role as secretary of the works council and her union membership had worked against her.

The respondent failed to prove the real reasons why it had departed from the algorithmic criteria, and the court therefore ruled that the company had indeed breached the fundamental right to freedom of association. As a result it held the appointment of one of the chosen candidates null and void and recognized the plaintiff's right to receive the difference in salary relating to the position to which she was legitimately entitled. In response to this ruling, the port authority filed an appeal, taking the case to a second instance for review, which ended by reaffirming that the plaintiff had suffered union discrimination.

In short, the ruling sets an important precedent in connection with guaranteeing fundamental rights in the workplace, particularly with regard to freedom of association and transparency in internal selection processes within public organizations.

The Supreme Court of Chile orders a telecommunications company to provide indemnification to a customer due to the breach of personal data

The Supreme Court of Chile ordered a telecommunications company to pay indemnification totaling seven million pesos to a customer whose identity was used by scammers to sign up for five telephone lines without his consent. The ruling held that the company had failed to fulfill its duty to protect the personal data of the person concerned, which had facilitated the fraud. The company was held responsible for failing to adequately verify the identities of the individuals who signed the contracts, in breach of the Personal Data Protection Law.

The ruling sets a precedent in the protection of personal data in Chile by imposing a penalty on the company for breaching the law and facilitating fraud.

Latombe case: The GCEU validates the EU-US international transfer scheme

The General Court of the European Union (GCEU) has issued a judgment in the so-called “Latombe Case”, involving an action for annulment brought by MEP Philippe Latombe against the US international transfer scheme that is currently in force.

One of the main points of this ruling hinged on the independence of the US Data Protection Review Court (DRPC), which acts as an appeals court in relation to data protection matters in that country. According to Mr. Latombe, the DPRC is not impartial or independent, due to its dependence on the executive. However, the GCEU held that the DPRC afforded a series of guarantees and had acted in accordance with certain rules that offered sufficient evidence of the functional independence of its members. As a result, together with other additional grounds, the GCEU dismissed the appeal.

With this ruling, the TGUE, generally ratifies the scheme, confirming that it offers sufficient guarantees to ensure an adequate level of protection for the data being transferred, which avoids — at least for the time being — a further annulment of the scheme for regularizing such transfers, as occurred with the former Privacy Shield and Safe Harbour systems.

In any event, as the GCEU observed in its press release on the subject, the European Commission must monitor the legal framework of data transfers to the US so that if any developments arise that impact on the applicable guarantees, the Commission may decide to amend or suspend, the scheme.

The National Appellate Court considers that requests for access to personal data must be sent to the channels set up for this purpose and not to generic addresses

The appellant had filed an appeal for judicial review at the National Appellate Court against a decision by the AEPD which had rejected his complaint that he had not received a response to his request for access to the personal and academic data processed by a university. The complainant had requested access to his academic record by sending an email to a generic address and after not receiving a response, he turned to the AEPD. The agency refused the claim on the grounds that the data subject had not used the specific channels provided by the university for the exercise of data protection rights, such as the email or postal address indicated in the university's privacy policy.

The National Appellate Court, in accordance with article 15 of the GDPR and article 13 of the LOPDGDD, confirmed the AEPD's decision. The Chamber held that the university had not limited or obstructed the right of access, since the complainant had not proven that he had submitted his request through the channels expressly provided and published by the institution for the exercise of rights. In this regard, it found that "it was the complainant who submitted his request outside the channels established for this purpose, failing to comply with the provisions in this regard on the website of the entity against which the complaint was filed."

It therefore dismissed the appeal, confirmed the AEPD's decision of inadmissibility, and ordered the complainant to pay costs, noting that the judgment was subject to appeal.

The CJEU analyzes the possibility of disclosing employee data from a company to its parent company to test software and declares the use of real data without a legal basis to be unlawful

The case involved the misuse of an employee's personal data by a German company belonging to an international group based in the US.

In 2017, the group implemented cloud-based human resources software for testing, stipulating in the contract that only limited data could be used (first name, last name, date of hire, place of work, and work phone number) and expressly prohibiting the use of real data for personnel management purposes. However, the company uploaded sensitive employee data to the cloud, such as salary, address, date of birth, marital status, social security number, nationality, and tax identification number, which were processed until 2019.

The employee filed a lawsuit at the labor courts, arguing that the use of real data was not necessary for testing purposes and that the permitted framework had been exceeded, requesting compensation for non-material damages. Both the first instance labor court and the regional court dismissed the claim.

Subsequently, the Federal Labor Court referred a question for a preliminary ruling to the Court of Justice of the European Union (CJEU) on the interpretation of article 88.1 GDPR in relation to German labor law. The CJEU noted that national law on data processing must comply in full with the conditions and limits in the GDPR, in particular articles 5, 6 and 9.

Finally, the Court concluded that the company had processed the personal data without a legal basis, in breach of article 6.1 GDPR, and awarded the employee €200 in compensation due to the loss of control over his data (article 82.1 GDPR). The court also underscored that the use of real data for testing purposes would only be justified if the dummy test data was not sufficient to achieve the purpose, which was not the case here.

The courts admit the use of video surveillance images as evidence in criminal proceedings

In its judgment of June 3, 2025, the Évora Court of Appeal Proc. 412/21.6JAFAR. E1, ruled on the admissibility of the use of images captured by a video surveillance system as evidence in criminal proceedings. At issue was the use of recordings obtained by cameras installed outside a nightclub, which captured a crime being committed. The court found that the images did not invade the heart of the defendant's private life and had been collected in a public place for the purpose of documenting criminally relevant facts, and were therefore admissible as evidence. The decision was based on the principle of just cause and the absence of a breach of the proportionality principle. The court found that the protection afforded by the GDPR, although applicable, did not in this context impose an automatic exclusion of evidence.

A judgment clarifies that consent by the data subject does not replace judicial authorization when it comes to providing evidence in the context of legal proceedings

In its judgment of April 30, 2025, Proc. 875/24.8PDVNG-A. P1, Oporto Court of Appeal addressed the possibility of using GPS location data installed in a motor vehicle in criminal proceedings. The case concerned a request made by the Public Prosecutor's Office to the telecommunications operator to obtain the location of a stolen vehicle. Although the contract holder had given his consent to the collection of the data, the operator refused to hand them over without court supervision. The court confirmed the need for authorization from the examining judge for validation of the evidence and for it to be included in the criminal proceedings, because the use of location data in criminal proceedings could interfere with fundamental rights, which requires prior judicial control. The decision clarified that the data subject's consent did not replace the requirement for court protection when the procedural admissibility of the data was at stake.

CNPD opinion on the online broadcasting of local authority meetings

The Portuguese Data Protection Authority (CNPD) issued Opinion no. 29/2025 on the online broadcasting of local authority meetings, at the request of the Parish Council of Avenidas Novas. The CNPD confirmed the understanding already adopted in 2023, and held that there were no legal grounds for the live online broadcast (audio and video) of these meetings, either based on the legal regime of the local authorities or on the principle of transparency set forth in the GDPR.

It pointed out that, although the publicity of the meetings was provided for by law, it did not involve their digital broadcast. Live broadcasting, by systematically exposing the images, voices, and opinions of participants, may violate the principle of minimization and represent a change in the purpose of the data collection. For this reason, the CNPD held that this type of broadcasting constituted additional processing that requires a new legal basis and, as a general rule, an impact

assessment, and underscored the need for strict compliance with article 13 of the GDPR, so that data subjects are fully and clearly informed of this processing.

The opinion acknowledged that the recording and subsequent availability of meetings could only be carried out based on the participants' consent, in accordance with article 6(1)(a) GDPR, provided that the requirements applicable to consent set out in the GDPR had been met in full. The CNPD had already pointed out that such consent must be obtained not only from those who, by carrying out their functions or exercising their right to participate, make statements during the meetings, but also from those who exercise the same right of participation simply by attending the meetings. Finally, the CNPD emphasized the need to distinguish between public officials, whose data may be subject to lower privacy expectations, and participating citizens, whose data requires greater protection.

In 2023, the CNPD had already published the guidelines on broadcasting local authority meetings online, on which the opinion issued was based.

5. News update

The EU Data Act has been applicable since September 12, 2025

Regulation (EU) 2023/2854, known as the *Data Act*, a key piece of legislation to achieve a more open and competitive data market in Europe, has been applicable since September 12, 2025. The regulation had entered into force in December 2023, but its general application begins now, with provisions affecting manufacturers of connected devices, cloud service providers, and all types of entities that manage data generated by the Internet of Things (IoT).

The Data Act establishes specific rights for users of connected products and services, guaranteeing them access to and reuse of the data generated by their devices. It also imposes obligations for fair data exchange between companies (B2B), enables restricted access by public bodies in cases of emergency or exceptional public interest, and promotes interoperability and portability in cloud services, with a gradual reduction in the costs of switching providers.

The Data Act establishes a progressive timeline for implementation. The general obligations of the regulation, such as those relating to transparency in data access and sharing, or contractual rules to prevent unfair terms in B2B contracts have been compulsory since September 12, 2025. Subsequently, as from September 2026, more specific technical requirements will come into force, such as the obligation for connected products and services to be designed so that users have direct access to the data. Finally, in 2027 certain provisions will also be extended to include previous long-term contracts.

At all times, the Data Act is applied in coordination with the General Data Protection Regulation, and it is expressly emphasized that the latter takes precedence, ensuring a balance between the data economy, technological innovation, and the safeguarding of privacy.

Click here to read the article "The Data Act comes into play: keys to a regulatory patchwork that businesses cannot ignore" by Begoña González Otero, of counsel in the Garrigues Intellectual Property Department and an expert in digital law.

The European Commission publishes a decision concluding that Apple and Meta are in breach of the Digital Markets Regulation and imposes fines of €500 million and €200 million, respectively

The Commission has issued a decision imposing a fine on Meta and Apple due to a breach of the Digital Markets Act (DMA).

In the case of Apple, the Commission determined that the company has breached its

obligation to allow app developers to inform users free of charge about alternative offers outside the *App Store*, as well as the possibility of redirecting them to those offers. A €500 million fine was imposed, as well as the obligation to remove all technical and commercial restrictions on redirection and to refrain from repeating the conduct in the future.

As far as Meta is concerned — this is where the decision most closely relates to the field of personal data protection — a penalty was imposed on the grounds of breach of article 5.2 a), b) and c) of the Digital Markets Act due to the use of the "consent or pay" system in relation to the processing of data for personalized advertising. It should be highlighted that the company has introduced a new model that is currently being reviewed by the Commission to determine its compliance with the law. Lastly, the Commission decided to impose a €200 million fine on Meta.

The EDPB publishes the Helsinki Statement and announces new measures to simplify and reinforce the application of the GDPR

The European Data Protection Board (EDPB) has published the **Helsinki Statement on enhanced clarity, support and engagement**, in which it outlines a series of initiatives aimed at facilitating the practical application of the GDPR and strengthening consistency in its enforcement throughout the European Union.

The main measures announced include:

- **Simplification of procedures**: preparation of reference templates for organizations, including a common template for reporting personal data breaches to data protection authorities.
- **Enhancing consistency**: the collection of positions by DPAs on priority issues and decisions in order to produce "case-law" style publications for organizations.
- **Cooperation with other regulators**: preparation of joint guidelines together with other regulators, to ensure consistency in the application of different legal frameworks.

With this statement, the EDPB seeks to respond to demands for greater regulatory clarity and practical support for organizations, while also promoting a consistent framework for GDPR compliance across the Union.

Chile: Implementation Commission for the new Data Protection Law publishes three reports

The Ministerial Advisory Commission for the Implementation of the Data Protection Law presented three reports this year with various recommendations for the implementation of this new law in the country. The first report looks at the Personal Data Protection Agency (APDP), recommends that it become operational by June 2026, and that its structure and budget should be strengthened to ensure the effective protection of personal data.

The second report focuses its recommendations on Chile's entry into digital value chains, encouraging innovation and ensuring the confidence of investors and trading partners. These include the approval of binding corporate rules submitted by companies and standard contractual clauses, as well as the exploration of international data transfer flows with APEC trading partners. It also addresses the declaration of countries that provide adequate levels of data protection, and indicates that the process of recognizing Chile as an adequate country and the process of accession to the Council of Europe's Convention 108+ should be initiated.

The third report directs its recommendations at the public sector and proposes that the Digital Government Department could issue a circular with guidelines and technical guidance to ensure coordinated implementation of the Data Protection Law in central government bodies. The priority measures include the appointment of data protection officers, the

creation of internal implementation committees, the adoption of processing policies and procedures for the exercise of ARCO rights, and the implementation of security measures and training plans.

The EDPB adopts guidelines 3/2025 on the interaction between the DSA and the GDPR

The European Data Protection Board (EDPB) adopted, on September 12m 2025, Guidelines 3/2025 on the interplay between the Digital Services Act (DSA) and the GDPR.

The EDPB emphasizes that the DSA pursues different and complementary objectives, does not repeal the GDPR, and does not itself create an autonomous legal basis for processing personal data: where compliance with the DSA involves data processing, providers must identify a basis under article 6 GDPR and observe the principles of minimization, purpose limitation, and proportionality.

The guidelines go into detail in sensitive areas. In the "*notice and action*" mechanisms and internal claims (arts. 16, 17, 20 and 23 DSA) only strictly necessary data should be processed and, where appropriate, the identity of the notifier should only be disclosed if essential, with adequate safeguards. In addition, automated decisions must comply with the restrictions of the GDPR, including those relating to special categories of data. In designs with dark patterns, the EDPB notes that article 25 DSA must be read in conjunction with the GDPR: consent and other choices regarding the processing of personal data cannot be manipulated; and advertising based on special categories of data is prohibited, even if, in abstract terms, there is a legal basis or an exception under article 9.2 GDPR.

For very large online platforms and search engines (VLOPs/VLOSEs), the EDPB underscores the DSA's systemic risk management together with data protection by design and by default and, where appropriate, data protection impact assessments (DPIAs) under the GDPR. It recommends avoiding age assurance mechanisms that enable unambiguous identification of users and permanently store their age, and calls for close cooperation between digital services coordinators, the European Commission and data protection authorities, as well as their involvement in the preparation of DSA codes of conduct to ensure consistency with article 40 GDPR.

AEPD Annual Report 2024: main results and trends

The AEPD has published its 2024 Annual Report and the overview is mixed: resolved claims have dropped, but both the total number of fines and the pressure to impose them in key sectors has risen. In 2024, 281 fines were imposed (−23% compared to 2023) for an aggregate amount of €35.6 million (+19%). The sectors with the highest fines were energy/water, financial institutions, internet services, telecommunications, and fraudulent contracting. The highest fine of the year, €5 million, was imposed for lack of transparency in the information provided to users, absence of a valid legal basis for certain processing operations, and deficiencies in compliance with the principles of lawfulness and fairness in the use of personal data.

In the area of personal data breaches, the Agency received 2,933 notices (+ 46% per year). 84% came from the private sector and 16% from the public sector, with more than 100 million people potentially affected. Breach-related proceedings accumulated more than €13 million in fines.

In terms of processing, the AEPD resolved 18,132 complaints in 2024 (−11% year-on-year). The role of data protection officer continued to gain ground: 206 officers were certified in 2024 (cumulative total of 1,306), with 11,227 officers reported, covering 119,803 controllers. Of these, 11.63% already have official certification. Finally, citizen services experienced strong growth, with 98,162 inquiries handled (+42.5%), reflecting increased demand for guidance on data protection.

The European Commission has published a report on the implementation of the EU Global Health Strategy

Following the entry into force of Regulation (EU) 2025/327 establishing the European Health Data Space (EHDS), the European Commission published a report on July 10, 2025, on the implementation of the EU Global Health Strategy [COM(2025) 392].

The report presents the main actions taken and progress made on priority issues for improving global health. In particular, it highlights the progress made in implementing the Global Health Strategy, which focuses on three main priorities: promoting health, strengthening health systems, and protection against health threats.

The report is addressed to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, and provides information on the measures taken, the results achieved, and the challenges in implementing the EU's global health strategy.

In particular, the report highlights the strengthening of health data governance. In this regard, it states that one of the objectives of the EU Global Health Strategy is to capitalize on the EU's pioneering role in the regulation of health data and digital certificates, using cloud storage for data exchange, data protection, and privacy. Therefore, one of the EU's objectives is to harness the potential of health data outside the EU, in line with the principles of the European Health Data Space, which aim to encourage stronger governance of health data and greater interoperability. One of the practical examples that helps to move towards this goal is the project launched by the WHO Regional Office for Europe and the European Commission, under the EU Health Program, to strengthen health information systems, data governance and the interoperability of health data in 53 countries in the WHO European region. This four-year project aims to improve the use and reuse of health data by healthcare providers, policymakers, and patients, as well as to improve the quality and interoperability of health information systems.

The strategy highlights efforts targeting critical global health priorities, detailing progress made and ongoing EU action in this area. In particular, along with this report, the respective annex was also published, presenting a non-exhaustive list of key actions for the implementation of the Global Health Strategy.

The Commission will remain committed to monitoring the implementation of the European Health Data Space and will have until March 2027 to adopt a series of key implementing acts setting out detailed rules for the implementation of Regulation (EU) 2025/327.

Joint report published by the AEPD and the European Data Protection Supervisor (EDPS) on the privacy implications of the use of federated learning in artificial intelligence

The AEPD and the EDPS have published a joint report on federated learning, a technique for training artificial intelligence models. This technique involves training models locally on each device and only sharing the result, without having to send the original data to a central server, which reduces the risk of leaks and unauthorized access. The report highlights applications in the healthcare sector, voice assistants, and autonomous vehicles.

The report reaffirms that federated learning is in line with principles such as data minimization and purpose limitation, and also reinforces proactive accountability and auditability. However, it cautions that it should not be assumed that the parameters exchanged are anonymous without a technical and legal analysis, as they could allow inferences about sensitive data. It also underscores the need to implement security measures throughout the ecosystem, ensure the quality and absence of bias in the distributed data, and protect the system from attacks that exploit the weakest link.

The European Data Protection Board (EDPB) publishes the final version of Guidelines 02/2024 on article 48 GDPR

Following a provisional publication of the guidelines on article 48 GDPR in relation to data transfers to third-country authorities, the final version has been published, with several changes with respect to the first version.

As explained in our April newsletter, the guidelines focus on requests for direct cooperation between a public authority in a third country and a private entity in the EU, emphasizing the need for such transfers to be covered by a lawful basis and by one of the mechanisms provided for in the GDPR for international transfers. Some nuances have been added to the final version, among which we will highlight the most relevant.

These guidelines are not applicable if the transfer request comes from a subsidiary or parent company of the group outside the EEA, even if it is supported by a request from the authority located in that country outside the EEA. In addition, it reinforces the idea that if the request is made by the authority to a data processor, the processor must inform the controller and follow their instructions, unless this is prohibited by law on the basis of an important public interest. Finally, it also adds that international agreements on which the transfer is based should allow the authorities to request information from private entities, and that it should not be merely a matter of cooperation between public authorities. In the event of doubt as to the existence of an international agreement and its content, the EDPB indicates that the national authorities (Ministry of Justice and Ministry of Foreign Affairs, among others) should be consulted.

Council and European Parliament reach deal to make cross-border GDPR enforcement work better for citizens

The Council and the European Parliament have reached a provisional agreement on a new legal act (which is expected to take the form of a regulation) to streamline and harmonize cross-border administrative procedures in the field of data protection, increasing cooperation between the supervisory authorities and thus improving the efficiency of the application of the GDPR.

In this regard, the new regulation recognizes several aspects, including the relaxation of the requirements for the complainant to be heard in complaint proceedings, and the regularization of deadlines for completing investigations (15 months, extendable to a further 12 months, except for simplified investigations, which must be closed within 12 months). Similarly, an early resolution mechanism has been agreed upon, allowing the data protection authorities to resolve a case before involving other foreign authorities.

A measure has also been introduced requiring the lead authority to send a summary of the key issues to its counterparts in the EU. Finally, a Council proposal for a simplified cooperation procedure has been maintained, consisting of the option not to apply all the additional rules for cross-border procedures when a case is more straightforward, which reduces the administrative burden on the authorities.

AEPD analyzes whether it is mandatory for an artificial intelligence system used in automated commercial communications to understand and implement privacy policies

The Spanish Data Protection Agency (AEPD) studied a case involving a company that sent automated commercial communications through an artificial intelligence system via instant messaging. The recipient of the messages claimed not to have given their consent and to be registered on the Robinson list, and requested that the messages cease. However, the company had established a clear and free procedure for objecting to the processing of data for promotional purposes, which consisted of replying with the word "unsubscribe." The AI system only recognized

that word and was not programmed to interpret other forms of objection. Despite the person's repeated requests to be removed, the system did not process their request because they did not use the exact term.

The AEPD highlights several key points:

i. Clear and free opt-out procedure: the company offered a simple method for objecting to the data processing (sending "unsubscribe"), which complied with data protection regulations.

ii. Limitations of the AI system: the agency considered that, although it would be desirable for AI systems to be able to interpret any human form of objection, it is not legally required that they be ready to do so. An automated system cannot be required to understand all the possible ways in which a person can exercise their rights.

iii. Information on the use of AI: the AEPD noted that, as of August 2026, it will be mandatory to expressly inform users that they are interacting with an AI system, although it currently only recommends this as good practice.

iv. Availability of other channels: it emphasized that the person could exercise their rights by other means, such as by email or on the website, and that human assistance was available to handle these requests.

In short, the AEPD considered that the company had complied with the obligation to offer a clear and free channel for exercising the right to object, and that the AI system was not required to interpret any message that was sent. Furthermore, the agency found that the existence of alternative channels for contacting human agents reinforced the company's position in terms of compliance with the legislation.

The AEPD responds to a prior consultation regarding the use of biometrics for access control at Civil Guard facilities

The AEPD has issued a response to a prior consultation based on article 36 of the GDPR in relation to the implementation of a biometric access control system at the facilities of a public security entity.

The proposed system does not generate a centralized database, but rather keeps the biometric template in the user's possession, which reduces the risks of mass processing. The purpose of the processing is the identification and access control of people, vehicles, and residents in sensitive facilities, based on several regulations such as Organic Law 7/2021, Organic Law 2/1986, and the GDPR.

The AEPD analyzed the legitimacy of the processing, highlighting that biometric data are special categories that require enhanced safeguards. It made a distinction between identification and authentication, and noted that the latter was less intrusive and more proportionate in controlled contexts. The system incorporates advanced technical measures such as the local generation of non-reversible identifiers, exclusive control by the data subject, non-centralized storage, and strict limitation to authentication purposes. These features minimize the impact on fundamental rights.

The AEPD concluded that the proposed biometric processing complied with the requirements of legality, necessity, and proportionality, and that there were no equally effective alternatives with less impact. However, it recommended that a different assessment be used in less critical areas, and that the possibility of using non-biometric alternatives be offered in certain cases. Finally, it underscored the importance of conducting periodic impact assessments, ensuring compliance with the National Security Scheme, and maintaining data protection under the exclusive control of the data subject, preventing misuse or access by third parties.

European Commission publishes guideline on the obligations of general-purpose AI models

The European Commission has published guidelines on the scope of the obligations applicable to providers of general-purpose artificial intelligence models (GPAI) under Regulation (EU) 2024/1689 (AI Act), which came into force on August 2, 2025.

The European Commission's guidelines on the Artificial Intelligence Regulation (AI Act) clarify the obligations that providers of general-purpose AI models must comply with, especially those with systemic risk. They establish technical criteria (such as training computation in FLOP) to identify these models, detail obligations for transparency, documentation, copyright compliance, and risk assessment, and provide exemptions for open-source models under strict conditions.

They also regulate supervision by the AI Office, notification and classification procedures, and the transitional regime until the full application of the penalty regime in August 2026.

The EDPB issues a statement on the non-binding model contractual terms of the Data Act

The European Data Protection Board (EDPB) has issued a statement on the non-binding model contractual terms (MCTs) to facilitate data sharing in accordance with article 41 of the Data Act.

The EDPB warns that these terms, although non-binding, must be brought into line with the (GDPR) when dealing with personal data. Its observations include, the need to clearly distinguish between personal and non-personal data, to improve the structure and definitions of the MCTs, and to ensure that contractual clauses do not prevail over data protection regulations in the event of a conflict.

It also points out that compliance with MCTs alone does not guarantee compliance with the GDPR, and that additional measures such as standard contractual clauses may be required for international transfers. It also recommends considering consumer vulnerability and avoiding disproportionate penalty clauses.

The EDPB remains available to continue collaborating on the improvement of these contractual instruments.

The EDPB contributes to the European Banking Authority (EBA) public consultation on draft regulatory technical standards (RTS) on anti-money laundering and countering the financing of terrorism (AML/CFT)

The EDPB indicates that, since the entities obliged to comply with AML/CFT obligations may be natural persons, this may entail the processing of personal data, and therefore a reference to the applicability of the GDPR should be included in the RTS.

It also makes a number of suggestions for amendments to the proposed RTS, such as:

i. To include an express reference to the obligation to have adequate technical and organizational measures in place under article 32 of the GDPR.

ii. With regard to remote identity verification, the processing of personal data should not be based on consent, as it is not optional for the customer to provide this information. The AEPD therefore suggests that the legal basis should be compliance with a legal obligation (article 6.1.c) GDPR).

iii. To clarify that the information stored must be updated and rectified without undue delay.

iv. To ensure that the principle of minimization is complied with in relation to the collection of personal data from third parties in cases of suspected criminal activity.

The AEPD and the Brazilian Data Protection Authority expand their institutional collaboration

In the context of the Global Privacy Assembly (GPA) held in Seoul, the president of the Spanish Data Protection Agency (Lorenzo Cotino) and the director-president of the Brazilian National Data Protection Authority (Waldemar Gonçalves) have signed the renewal of the Memorandum of Understanding (MOU) between both institutions. This agreement strengthens institutional collaboration and establishes a framework for the creation of joint actions aimed at the promotion and practical application of personal data protection.

The MOU provides for the exchange of technical knowledge, cooperation in research, studies, and analysis, as well as the development of guidelines and tools to facilitate regulatory compliance. It also envisages the creation of joint initiatives, especially in the context of international programs and projects.

In the Ibero-American sphere, it highlights the joint work being carried out in the Ibero-American Data Protection Network, a forum currently chaired by the ANPD, with the Spanish Agency acting as permanent secretary. Recent achievements include the approval of the "Ibero-American Data Protection Standards," which encourage the adoption of mechanisms for the exchange of best practices and experiences among the countries in the region.

This agreement consolidates international cooperation and the leadership of both authorities in the protection of personal data at a global and Ibero-American level.

Researchers from the European Commission's Joint Research Centre publish an article on 'AI Benchmarks'

The article analyzes the problems and limitations of benchmarks or reference indicators in artificial intelligence (AI), which have become key tools to evaluate the performance, capabilities, and risks of AI systems and are increasingly relevant for both research and regulation, especially in the context of the implementation of the AI Act. In this regard, the study starts out with the premise that, although benchmarks allow models to be compared and progress to be measured, their widespread use has raised concerns about their suitability for assessing sensitive aspects such as the safety, social impact, or systemic risks of AI.

The article concludes that current benchmarks, which are mostly quantitative and performance-oriented, are insufficient to provide the guarantees of safety and reliability demanded by legislators and society. The authors therefore recommend requiring greater transparency and documentation in the creation and use of benchmarks, promoting diversity and inclusivity in their design, developing dynamic and multimodal benchmarks that better reflect the actual risks and capabilities of AI systems, and establishing rigorous validation and updating protocols.

In addition, they advocate evaluating not only performance, but also the errors, weaknesses, and unintended consequences of the models, and creating mechanisms to assess the reliability of the benchmarks themselves, beyond their popularity or the number of citations.

The UK Information Commissioner's Office (ICO) publishes an article on how to ensure effective anonymization of personal data

The article provides guidance on the effective anonymization of personal data, offering a practical and strategic approach to ensuring that this process is carried out effectively, allowing entities to process data without compromising user privacy.

In order to assess whether a dataset has been effectively anonymized, the ICO proposes applying the so-called *"motivated intruder test*." The test consists of analyzing whether a

person with reasonable motivation, knowledge, and resources could identify a user using the anonymized data together with publicly available information. If there is a significant probability of identification, the data cannot be considered anonymous.

In addition, the guide emphasizes that anonymization must be effective not only for the data controller, but also for any third party that has access to the data. Similarly, the ICO recommends that organizations should adopt a strategic and technical approach by proposing data protection impact assessments (DPIAs) where necessary and carefully documenting the decisions and measures taken. The guide provides practical steps for identifying risks, applying appropriate anonymization techniques, and establishing controls that strengthen information protection.

Finally, the article concludes by highlighting the numerous benefits of implementing the measures outlined, which allow data to be shared and reused with fewer legal restrictions, encourage responsible innovation, and improve transparency for stakeholders. They also reduce the regulatory burden by excluding anonymized data from the scope of the UK GDPR, which, according to the ICO, could facilitate analysis, research, and technological development projects.

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

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

Adrián León
Associate · Alicante
adrian.leon@garrigues.com

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

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

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

Manuel Liberal Jerónimo
Partner · Lisbon and Porto
manuel.liberal.jeronimo@garrigues.com

Sebastián Hassi
Principal associate · Santiago de Chile
sebastian.hassi@garrigues.com

Antonio Durán
Associate · Malaga
antonio.duran@garrigues.com

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

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

Matilde Bettencourt
Associate · Lisbon
matilde.bettencourt@garrigues.com

Further information:

Data Economy, Privacy and Cybersecurity

GARRIGUES

Plaza de Colón, 2
28046 Madrid
T +34 91 514 52 00
info@garrigues.com

Follow us on: