GARRIGUES

# Data Economy, Privacy and Cybersecurity Newsletter

June 2025

# Contents

# 1. Proposal by the European Commission to amend the GDPR: a critical review and practical suggestions

**The European Commission has recently presented a proposal to amend the GDPR with a view to reducing the bureaucratic burden on small and medium-sized companies. The main measure that has been introduced is to expand the exceptions to the obligation to keep a Record of Processing Activities ("RoPA"). Although the intention behind the amendment is positive, the approach taken has been criticized because it fails to bear in mind the essence of compliance with the Regulation. We analyze what this implies (not necessarily an improvement for small and medium-sized companies) and propose various alternatives to facilitate compliance with the GDPR.**

**Alejandro Padín Vidal**

The European Commission has recently published a proposal for a regulation that aims to simplify certain obligations affecting micro, small and medium-sized enterprises. The measures addressed in this document include a proposal to amend the General Data Protection Regulation (GDPR). The spirit underlying this proposal is, principally, to simplify compliance with some of the obligations of the GDPR, supposedly with the aim of helping small and medium-sized companies to adhere to the Regulation by reducing the bureaucratic burden, in order to save costs and increase business efficiency.

Although the aim and intention are commendable, the content of the proposals could miss the mark since they focus on certain aspects that are worlds away from the problem faced by SMES in adhering to the GDPR.

In this article we give specific examples and propose certain changes that could prove useful to improve the situation of compliance and adapt it to the reality faced by small and medium-sized businesses.

## 1. Obligation to keep a Record of Processing Activities and the exceptions

The main measure of the Commission's proposal refers to the obligation in article 30 of the GDPR to keep a Record of Processing Activities (RoPA). Specifically, the proposal seeks to extend the threshold of exceptions that are applicable to this obligation, so that a greater number of businesses can decide not to keep a record.

The current wording of article 30, paragraph 5, of the GDPR contains the following exceptions:

*The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offenses referred to in Article 10.*

The text is clearly binding on all businesses with over 250 employees and also those with fewer numbers in any of the following three circumstances: (i) if the processing involves a risk, (ii) that is not occasional or (iii) that includes special categories of data or regarding criminal convictions.

The current text of article 30.5 is to be replaced with the following:

*"The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organization employing fewer than 750 persons unless the processing it carries out is likely to result in a high risk to the rights and freedoms of data subjects, within the meaning of Article 35".*

As can be seen, in addition to the increase in the employee threshold, two of the three instances in which small companies must also keep a RoPA are also eliminated, namely that the processing is not occasional or that it includes special categories of personal data.

A reflection on this proposed amendment raises the following questions: does not having a RoPA, actually relieve the bureaucratic burden? Does it make it easier for small companies to comply? Will it improve the level of compliance?

## 2. Comments on the proposed amendment

In our opinion, the proposed change poses doubts for two reasons: firstly because it does not bear in mind the origins of the current article 30.5 and the reasons why a numerical criterion was included in the text. Secondly, because it does not take into account the essence of what the RoPA means in a program of compliance with the GDPR and is misleading for obliged entities as to the most essential aim of the GDPR.

### a. Increase in the number of employees

Regarding the first reason, we need to take a look at how the GDPR evolved over the four years that the legislation process lasted at the EU institutions until it was finally approved and published in the Official Journal of the European Union (OJEU) as as compulsory legislation.

In this regard, it should be borne in mind that in some of its initial versions, the draft GDPR contained several cases in which certain obligations were linked to different types of numerical criteria (for example, in the initial version of the proposed GDPR, the obligation to designate a Data Protection Officer (DPO) or representative at the EU was linked to the organization employing over 250 persons; subsequent versions linked it to the existence of processing that affected over 5,000 data subjects; these objective barriers were finally dropped). Against this background of objectively establishing obligations, article 30 introduced the obligation for businesses with over 250 persons to keep a RoPA. In this case, as opposed to others in which the numerical references were eliminated, the figure was maintained.

During the passage of the GDPR through the European institutions, it swung between a legal approach based mainly on the Napoleonic Code system, of an administrative nature (continental European law) and the Common Law approach, with an element of "accountability").

"Accountability" is a legal concept that does not have a direct translation into Spanish. The Spanish version of the GDPR translates it as "*responsabilidad proactiva*", whereas the AI Act translates it as "*rendición de cuentas*". The full content of "accountability" includes: (i) the obligation to fulfill a specific obligation, (ii) to be able to demonstrate compliance at all times, and (iii) accountability or responsibility in the event of non-compliance with either of these two obligations.

The final result was a hybrid regulation that includes articles that represent both legal systems. For example, articles 13 and 14 (obligation to provide information), article 28 (content of the processor agreement) and article 30 (RoPA) provide a clear representation of heavily administration-oriented tradition, whereas articles 5.2 (accountability principle), article 25 (privacy by design and by default) or article 32 (security of processing) are clear examples of Common Law.

The final review and the consensus that needed to be reached to be able to publish a regulation that was accepted by all, was not an easy task. The political agreement reached clearly involved removing the objective references to compliance and replacing them with a more flexible approach, in line with the case in hand, applying risk analysis criteria. The references indicated were eliminated (number of employees or processing for DPO, number of employees or data subjects affected for a representative in the EU, etc..) and replaced with specific obligations or uncertain legal concepts, because it was considered that adherence to the provision should not be established in terms of thresholds, but rather that the most important criterion was the risk for the rights and freedoms of the data subjects whose data were being processed. The risk of processing for persons obviously doesn't depend either on the number of employees at the organization processing the data, or on any other objective criterion. The data processing carried out by a company with 1,000 employees can involve less risk than the processing carried out by a company with 25 employees.

In this final task of eliminating numerical thresholds, the threshold in article 30.5 of the GDPR cannot be classed as a last-minute oversight, because the advisability of keeping a RoPA has nothing to do with the number of persons employed by the organization. In any event, even if that wording was not an oversight, the text itself does not include sufficient "exceptions to the exception" which, in practice, means that the RoPA is an obligation in the vast majority of cases, bearing in in mind the extent to which technology is used nowadays.

Therefore, the increase in the number of employees needed to keep a RoPA is hard to understand.

### b. Doubts regarding the greater flexibility in general

The second observation regarding the approach of the proposed modification with regard to the obligation to keep a RoPA, hinges on the essence of what a RoPA actually is and its place in the scheme of adherence to the GDPR. We should not lose sight of the fact that proposal has emerged seven years after the compulsory application of the Regulation, when we now have sufficient experience and practical and legal criteria to understand what a RoPA actually is, its importance and what it means.

As we have seen, in addition to the numerical criterion regarding the employees, the proposal eliminates the obligation to keep a RoPA where the processing entails a risk to the rights and freedoms of the data subjects (it is replaced with "a high risk"), where the processing is not occasional and where special categories of data are processed.

It should be borne in mind in this regard that the RoPA can be classed as the backbone of a program of compliance with the GDPR. This is because, more than simply a formal obligation to draft a document, a RoPA constitutes a detailed inventory of the data processing carried out by the data controller. This is, in turn, essential in order to comply with many of the other obligations of the GDPR. The most immediate is the obligation to provide information (article13), which requires the

data controller to provide the data subject with all the important information affecting the processing. These points are listed in detail in the RoPA and for this reason, drafting a privacy policy without a RoPA becomes an unwieldy and abstract task. A RoPA is equally important in relation to the verification of data storage obligations, security measures, international transfers, the control and monitoring of data processors and data disclosures. This is all reflected in the RoPA and serves as a guide to adhere to the GDPR.

Anyone who has rigorously prepared a GDPR compliance project knows that without the RoPA, the task is much more complicated. This is why it is surprising that increasing the number of cases in which it is not necessary to have a RoPA is considered a "measure to bring in flexibility". The consequences, far from bringing in flexibility and reducing red tape, can only be a deterioration in the extent to which SMEs comply with the GDPR and greater difficulty in achieving a good program of coherent and orderly compliance. Companies that qualify for these exceptions could be lulled into a false sense of security as to their compliance and will find it more difficult to adhere fully to the GDPR. It could also increase the number of companies that are falling into the hands (ever more often) of unscrupulous advisors who sell photocopied paper without valid content (since a RoPA is not needed, it is easier for a program devoid of content to be overlooked by someone without knowledge of the subject).

## 3. Proposals to improve the GDPR

Consequently, the GDPR does not need to be made more flexible as far as the RoPA is concerned. We will now look at which measures could actually prove useful to help SMEs comply with the Regulation and, in short, better protect the rights and freedoms of the data subjects (which is what really matters).

From the experience gained in the nine years that have passed since the publication and entry into force of the GDPR in 2016 and the 7 years of mandatory compliance since May 25 2018, there are several improvements that could be made, even without the need to change a single comma of the GDPR. Some examples:

- **To promote, more efficiently, the publication of codes of conduct or certification schemes.** The proposed amendment of the GDPR propounded by the Commission, also includes, as second and third measures, the inclusion of a specific reference to mid-cap enterprises in addition to the SMEs that already existed in the articles setting out the possibility of approving codes of conduct and certification schemes. However, what is actually needed, is for their creation to be actively encouraged, for example by publishing content templates for codes of conduct that industry associations can use as a reference.

- **To develop documentation that enables compliance with data transfer impact assessments (DTIA).** At present, it is extremely frustrating to see how countless companies are forced to repeat the same analysis carried out hundreds of times before by other companies. It means they have to spend a small fortune to obtain a report that could well have been prepared by one of the competent public authorities. For example, although a DTIA requires various inputs - some specific to the case in question - the truth is that many others refer to the analysis of the legal system and the application of the law in the country receiving the data. Making each company that is going to perform an international transfer to a particular country based on standard contractual clauses (the vast majority) commission a legal report on that country, is an unfair and disproportionate bureaucratic and economic burden. Indeed, this burden could be eliminated entirely by means of a single report prepared by a national or European institution in each country. Needless to say, eliminating the RoPA will not reduce this real and everyday problem.

- **To simplify the interpretation of the Regulation through the implementation of effective and useful consultation channels by the supervisory authorities.** To focus supervision on a constructive discussion process between the authority and the controller so that progress can be made in compliance beyond penalty proceedings. In addition, to make sure that companies are not afraid to approach the authorities and make them feel confident that they are going to receive assistance and not silence or evasive answers.

- **To support and help companies that suffer cyberattacks improve their situation as regards information security**. In most cases, if not all, despite having invested in cybersecurity, businesses are helpless in the event of a cyberattack and to make matters worse, this also involves a penalty from the supervisory authorities. The penalty system should be the "last resort" in the application of the GDPR, reserved for those clear cases of willful or recalcitrant breach and not for those cases in which businesses suffer unwanted situations even though they have tried to comply.

In closing, the amendments made to the GDPR, which seek to make it more flexible and improve efficiency at companies without weakening the protection of personal data, should be welcomed and encouraged. However, it might perhaps be easier to reflect on how to achieve these same objectives without changing the Regulation (which was so difficult to approve and is so resolute), addressing the practical problems in its application and facilitating its real and effective compliance by the entities that are subject to it.

# 2. Data protection authorities' decisions

## The AEPD imposes a penalty in the case of SIM swapping

The AEPD (Spanish Data Protection Agency) has imposed a total fine of 1,200,000 euros on a telecommunications company as a result of two infringements due to a breach of article 6 of the GDPR, relating to legal bases (200,000 euros), and article 25 of the GDPR, on data protection by design and by default (1,000,000 euros).

This penalty arose in a case of SIM swapping, in which certain workers at the sanctioned entity perpetrated this fraud at the store where they worked. The decision states that the controller had in place a number of internal procedures relating to data processing by its staff, which included the necessary implementing measures. However, the AEPD considered that this documentation was general in nature, given that, although it referred to the existence of risks, they were not sufficiently described, nor were specific actions established in the event that they materialized.

After rejecting the various submissions made by the sanctioned entity – which, among others, argued that the AEPD was assuming a strict liability standard, based on an analysis of results – the AEPD concluded that the entity's organizational measures were not sufficient, particularly taking into account that this type of fraud is relatively common in its sector and may have very serious consequences for data subjects.

As a result, the AEPD imposed a penalty for both the processing without a legal basis per article 6 of the GDPR and for the breach of article 25 of the GDPR, in a lengthy decision of great interest, mainly due to the observations made regarding the level of due care that data controllers must adopt in complying with the principle of data protection by design and by default.

## La Liga sanctioned with a million euros due to processing of biometric data

The AEPD has imposed a €1 million penalty on the Spanish professional football league (Liga Nacional de Fútbol Profesional or "LNFP") due to an infringement of article 35 of the GDPR and has ordered a temporary or definitive limitation on the processing of the biometric data of fans at clubs where access control is conducted with this technology, until a valid data protection impact assessment (DPIA) has been performed and passed.

The penalty was due to the LNFP's failure to perform a DPIA on the processing of biometric data for access to the stands at first- and second-division football stadiums, in breach of article 35 of the GDPR. According to the AEPD, the LNFP was responsible for

conducting this assessment due to its role in installing the biometric control access system.

The AEPD noted the lack of care on the part of the LNFP, given that, despite the information available on the risks associated with biometric data processing, this entity imposed a system that required sports clubs and corporations to process biometric data for access to the stands. In addition, through a subsidiary, the LNFP created technical means to implement the biometric system, thereby influencing access requirements and obliging the clubs to adopt a specific technical solution, without having performed the DPIA.

## The AEPD fines a mutual society 600,000 euros for a security breach that affected nearly 3,400 people

The AEPD's decision in proceeding EXP202412881 referred to a security breach committed by a mutual society authorized by the social security system, which affected 3,395 people whose personal data, including health data, were sent by mistake to 354 unauthorized entities. The incident took place in the context of the use of an online platform that enables associated enterprises and consultancies to receive weekly emails containing Excel files with information on their workers' financial benefits.

The technical failure that caused the breach was due to a modification in the automated notification system, whereby an essential line of code was deactivated by mistake. This line served to prevent the accumulation of prior addressees' files in subsequent dispatches. Since it was not executed, emails sent to the entities contained not only the relevant files, but also others that did not pertain to them, which triggered a massive exposure of personal data.

The mutual society detected the error after being alerted by a user company and proceeded to correct the code, implement technical controls and contact the recipient entities to request the deletion of the data, as well as to report the breach to the AEPD. It also proposed a redesign of the system with enhanced measures relating to the security, traceability and automatic expiration of documents.

The AEPD considered that the mutual society violated the integrity and confidentiality principle of article 5(1)(f) of the GDPR, since it did not apply the appropriate technical and organizational measures to ensure the security of the personal data. The infringement was classified as very serious, in accordance with article 83(5) of the GDPR and article 72.1.a) of the LOPDGDD. The AEPD initially proposed a penalty of 1,000,000 euros, which was reduced to 600,000 euros after the mutual society acknowledged its liability and paid the penalty voluntarily, which concluded the penalty proceeding.

## The right to be forgotten is denied with respect to publicly accessible information linked to public employment

In proceeding no. EXP202404813, the Spanish Data Protection Agency issued a decision in a case concerning rights, which commenced with a claim against a well-known online search engine company, where the claimant sought the deletion of several links that appeared in the search engine's results when his name and surnames were introduced. The claimant argued that the links contained obsolete personal information concerning his professional career and with no public relevance, and that its continued publication infringed article 93 of the LOPD-gdd regarding the right to be forgotten.

The respondent argued that part of the URLs had already been subject to a prior decision rejecting the right, that others did not appear in the search results and that the rest referred to institutional information regarding selection processes and appointments as a tenured civil servant. It asserted that this information was publicly relevant and that its publication arose from statutory obligations concerning active transparency and disclosure.

The AEPD concluded that the personal data published arose from administrative acts

linked to selection processes governed by the principles of merit, capability, equal treatment and disclosure. It considered that preventing search engines from redirecting to this information would be detrimental to the disclosure principle that governs access to public employment. It also indicated that the time elapsed since publication (2021 and 2022) was insufficient to consider the information as obsolete, particularly when the claimant was still a tenured civil servant.

Therefore, the AEPD dismissed the claim on the grounds that there were no circumstances that would justify the prevalence of the claimant's right over the public interest in retaining the links.

## A company is sanctioned for using employees' personal WhatsApp accounts for work purposes

The Spanish Data Protection Agency resolved the penalty proceeding commenced against a company following a claim by a worker who reported that customers' personal data were being sent to his personal WhatsApp repeatedly, despite the fact that he had expressly objected to the use of his personal device for such purpose. The company argued that the use of WhatsApp was a common practice agreed to by all employees and that the claimant had also initiated communications using this channel.

In its decision the AEPD concluded that the company had infringed article 6(1) of the GDPR by processing the claimant's personal data without a legal basis, even after the employment relationship had ended, and article 32 of the GDPR because it did not apply the appropriate security measures when sending customer data to a private device the settings of which it could not control. The AEPD dismissed the company's submissions, noting that neither the custom nor the alleged tacit acceptance justified the processing, and that the claimant had reiterated his refusal to use his personal cell phone as a work tool.

Two financial penalties were imposed: one of 2,500 euros for the infringement of article 6(1) of the GDPR and another one of 2,500 euros for the infringement of article 32 of the GDPR. In addition, the company was ordered to evidence within three months that it had adopted measures to avoid contact with former workers without a legal basis and to ensure that customer data are not sent to personal devices without complying with the requirements of the GDPR and the LOPD-gdd.

## Double penalty totaling 3,500,000 euros imposed on a bank for not ensuring the security of its clients' personal data

In decision PS 00477-2023, a claim was filed by two individuals against a bank when it was found that the mother of one of the claimants had unauthorized access to the financial information relating to the claimant's bank accounts. In the case examined, the mother appeared as an authorized party in two accounts held solely by one of the claimants, but the online banking operating system allowed her to view information relating to the shared accounts and all of the associated products such as credit cards, mortgages and insurance, without being authorized to do so.

The claimant submitted several internal complaints to the bank and the Bank of Spain without obtaining a satisfactory solution. The bank initially acknowledged that there was a "technical incident" that allowed the claimant's mother to access the unauthorized information.

The AEPD determined that the company had infringed several articles of the GDPR, including the failure to obtain express consent and the absence of adequate measures to ensure the security of the data. The AEPD held that there had been "negligence in the processing of the data", given that, despite being aware of the facts reported by the claimant, the necessary measures had not been adopted to stop the infringement continuing. For this reason, the respondent's conduct was considered to be even more negligent and unlawful.

The decision concluded with the imposition of a financial penalty on the infringing company, as well as the obligation to adopt corrective measures to comply with the data protection regulations. The facts constituted a dual infringement, attributable to the respondent, for infringing articles 5(1)(f) ("confidentiality principle") and 25 of the GDPR ("application of appropriate technical and organizational measures"). The balance of the circumstances envisaged with respect to the infringements committed allowed the AEPD to impose a fine of 500,000 euros for the first breach and another of 3,000,000 euros for the second one.

## A fine of 500,000 euros is imposed for the failure to inform the data controller of the identity of the entities to which services were intended to be outsourced

On April 1, 2009, the Regional Ministry of Universal Health and Public Health of the Valencia Autonomous Community Government signed a contract for the provision of healthcare services in the Health Department in Denia with a healthcare services association. The contract included a data processor agreement that established the obligation of the data processor to inform the data controller of the identities of the companies to which the services covered by the contract were intended to be outsourced. In view of the breach of this obligation, the Regional Ministry filed a complaint with the AEPD.

In this case, there is no record of the respondent having informed the Regional Ministry prior to the execution of the contracts signed with the sub-processors so that, as the data controller, it would have had the opportunity to object. When deciding on the amount of the administrative fine, the AEPD took into account the nature, seriousness, and duration of the infringement for failing to report the three contracts signed with sub-processors in 2018, which are still in force today, and the fact that the personal data affected by the infringement are health data, which are considered special categories of data. In view of the above, the penalty imposed amounted to 500,000 euros.

## A bank is fined for failing to implement the appropriate measures to ensure the confidentiality of personal data

On October 28, 2022, the AEPD received a security breach notification from the Spanish branch of a French bank, stating that one of the sub-processors engaged by that entity had suffered a ransomware cyberattack. In its decision in the penalty proceeding, the AEPD highlighted the following issues:

1. Regarding the Spanish branch's lack of standing to appear as a respondent and the lack of territorial jurisdiction of the AEPD, it considered not only the respondent's direct liability in the facts, but also that the agency has sufficient power to decide on the processing carried out in Spain.

2. As for the submission that the bank is a victim of a crime, the AEPD indicated that the respondent's fault cannot be deemed to have been excluded or mitigated by the fact that fraudulent conduct by a third party has taken place, since its liability does not stem from the third party's conduct but rather from its own conduct.

3. Regarding the obligations set out both in article 5(1)(f) and article 32 of the GDPR, concerning the need to apply appropriate technical and organizational measures to ensure a level of security appropriate to the risk which includes, among others, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services and the ability to restore access to personal data in a timely manner, the AEPD found that there was a lack of care in and suitability of the measures adopted and implemented by the entity in this specific case, particularly taking into account the varying likelihood and severity of the risks for the rights and freedoms of natural persons.

4. In particular, the AEPD found that third-party access would not have occurred if the personal data had been encrypted, pseudonymized, or anonymized, as the attacker would have obtained unintelligible information.

As for the data processor's liability, the AEPD noted that the bank is responsible for the personal data regardless of any liability that third parties unrelated to it may have incurred. In view of the above, the Agency imposed a penalty of 200,000 euros.

## A financial institution is fined 2,000,000 euros for demanding a client's consent to the processing of their data as a requirement to open a bank account

In its decision PS/00531/2023, the AEPD imposed a €2,000,000 fine on a financial institution which, for its customers to be able to conclude a contract to open a certain type of bank account, required them to grant their consent so that the bank could ask the Social Security General Treasury for information on their economic activity so as to comply with the provisions of Anti-Money Laundering and Counter-Terrorist Financing Law 10/2010, of April 28, 2010.

This law sets out the obligation to verify the professional and business activities of the parties with which business relationships are going to be established, but it does not stipulate that it should be done in a specific manner. Although consent can be opted for, the AEPD considered that the implementation was not appropriate, since consent cannot be considered a valid legal basis if the conclusion of the contract is subject to its being granted.

## The Irish supervisory authority for data protection fines TikTok 530,000,000 euros for making unlawful international transfers

The Irish supervisory authority issued a press release on May 2, 2025, in which it announced the imposition of a €485,000,000 fine on TikTok for making international transfers to China without a suitable assessment of the impact of these transfers, which made it impossible to adopt appropriate safeguards.

Furthermore, although the breaches detected in the privacy policy aimed at data subjects in the European Economic Area in the context of the inquiry were remedied by TikTok in 2022, the supervisory authority imposed a fine of 45,000,000 euros on TikTok for failing to comply with its obligation to provide information during the period from July 29, 2020 to December 1, 2022.

The two penalties amount to a total of 530,000,000 euros and include the obligation to bring the transfers into compliance within the next six months or otherwise the transfers will be suspended.

## The AEPD sanctions the Ministry for the Ecological Transition and the Demographic Challenge (MTERD)

The Fundación Éticas Data Society lodged a complaint with the AEPD alleging that the "BOSCO information system" used by the MTERD to determine whether to grant energy assistance relief makes automated decisions without significant human involvement, without periodic quality controls or adequate mechanisms for data subjects to challenge or express their point of view. It also highlighted the lack of transparency in relation to the information provided to data subjects about the processing and the absence of a data protection impact assessment (DPIA).

Despite the fact that the Ministry argues that there is human participation in the management of requests and in the processing of complaints, as well as the implementation of observation codes to report the reasons for rejection, the AEPD, in its decision of May 9, 2025 PS-00324-2025, stated as follows: (i) article 22 GDPR has been infringed, since the BOSCO system adopts automated decisions on the granting of energy assistance relief without complying with the required conditions; (ii) infringement of article 35 GDPR, for not carrying out a DPIA; and (iii)

infringement of article 13 GDPR, for not informing the data subjects of the existence of automated decisions or of their associated rights. Consequently, the AEPD imposed a series of corrective measures, including the obligation to inform data subjects of automated decisions and to carry out a DPIA within six months, as well as to guarantee the right to human involvement within nine months.

## The AEPD sanctions the General Council of Notaries (CGN) for requiring and storing a copy of the Spanish national I.D. card of registrants in the Notarial Citizen Portal

The claimant filed a complaint with the AEPD alleging that the Notarial Citizen Portal required a photograph of the Spanish national I.D. card on both sides in order to register, which the claimant considered excessive and unnecessary, as the electronic signature was sufficient.

In its decision of May 6, 2025 PS-00052-2024, the AEPD held that the processing was unlawful and article 6(1) GDPR had been infringed, since: i) although the notary is obliged to verify the documentation that proves the identification of the data subject (such as the Spanish national I.D. card ), its storage is only mandatory in the cases established in Anti-Money Laundering and Counter-Terrorist Financing Law 10/2010; and (ii) the consent obtained did not meet the requirements of the GDPR to be considered valid. Additionally, the AEPD noted that the CGN did not comply with the duty to provide information contained in article 13 of the GDPR, because the privacy policy did not suitably differentiate the legal bases or the purposes of the processing (particularly in relation to the storage of the copy of the Spanish national I.D. card). Lastly, the AEPD stated that the Data Protection Officer (DPO) of the CGN, which is the Notarial Certification Agency (ANCERT), breached the duty of independence required by article 38(6) GDPR, since he acted simultaneously as a data processor and a DPO, which entails a conflict of interest. Consequently, the AEPD ordered the adoption of corrective measures to bring the data processing into line with the applicable regulations and to evidence such circumstance within six months.

## Pharmacy fined 16,000 euros for three infringements of the GDPR

The pharmacy collected and stored patients' personal and health data (name, surnames, autonomous personal identification code (CIPA), personal identification code (CIP), medication, prescribing physician, health center, etc.) in excel files to renew medication without the presence of the patient or their health card. This processing was carried out without sufficient guarantees of protection, since the files were stored on the desktops of the pharmacy computers, protected only by a password common to all employees, and the computers were on counters visible to customers. In addition, the processing was carried out without the patient's informed consent, as no specific information was provided about the processing of the patient's personal data.

In its decision of May 5, 2025 PS-00187-2025, the AEPD imposed a total fine of 16,000 euros for the infringement of articles 13, 9 and 32 of the GDPR. Regarding the duty to provide information (art. 13 GDPR), the AEPD considered that the pharmacy did not provide information to data subjects on the processing of their personal data, thereby violating the principle of transparency, for which it imposed a fine of 3,000 euros. As to the processing of health data (art. 9 GDPR), the AEPD understood that health data were processed without an appropriate legal basis, without express consent or the occurrence of any of the exceptions contained in article 9(2) GDPR, for which it imposed a fine of 10,000 euros. With respect to the security of the processing (art. 32 GDPR), the AEPD considered that appropriate technical and organizational measures were not adopted to ensure the security of the data, and that there was potential unauthorized access and a lack of control over the files, for which it imposed a fine of 3,000 euros.

After notification of the decision initiating the proceeding, the pharmacy acknowledged liability and paid the penalty voluntarily.

## Sanctioned for improperly complying with the travelers' registration obligation

The claimant reserved a tourist apartment via a platform and was required to use an online check-in app that required taking a photo of both sides of the Spanish national I.D. card and sending a selfie to gain access to the accommodation. In its decision of May 8, 2025 PS-00546-2024, the AEPD imposed a total fine of 2,500 euros, which breaks down as 1,000 euros for infringement of article 5(1)(c) GDPR and 1,500 euros for infringement of article 9 GDPR.

Regarding the principle of data minimization (art. 5(1)(c) GDPR), the AEPD concluded that the sectoral regulations require the collection and communication of certain data (name, surnames, document number, nationality, date of birth, etc.), but not a complete image of the Spanish national I.D. card or a photograph of the guest's face, so there was no justification for this processing of personal data. As for the processing of biometric data (art. 9 GDPR), the AEPD considered that, given that facial biometric verification constitutes a processing of special category data (prohibited unless one of the exceptions of art. 9(2) GDPR is met) and none of the exceptions of article 9(2) GDPR had been met, there had been a processing of biometric data without a legal basis. In addition, the AEPD clarified that the legal obligation to register travelers does not cover the collection of excessive data or the processing of biometric data, as identity may be verified by other less intrusive means.

## The Polish Data Protection Authority issues a €132,000 fine because the DPO of a company did not fully exercise his independence and did not include profiling in the RoPA or in the DPIA

In its decision of November 18, 2024, the Polish Supervisory Authority imposed a €132,000 fine on a bank for infringing articles 30, 35 and 38 of the GDPR. Following an investigation, the Supervisory Authority found that, although the bank carried out profiling of numerous customer data for the purpose of determining their creditworthiness and subsequently processed the result of the credit score obtained, such processing was not entered in its record of data processing activities. In addition, the bank did not carry out a data protection impact assessment and, therefore, did not assess the implications of profiling for the security of the processing of personal data. However, the bank remedied this breach before the investigation was initiated.

The inspection also revealed the existence of a conflict of interest in the role of the Data Protection Officer (DPO) appointed by the bank. The DPO did not fully exercise the independence required by the GDPR because he did not report directly to the most senior management of the bank, i.e. the Board of Directors, and, in addition, he worked as an IT auditor/security specialist in the security department, reporting directly to the director of that department.

## The AEPD imposes a fine of 10,000 euros on a cosmetics brand for infringement of article 22.2 of the LSSI

The proceeding PS-531/2024 was initiated by a complaint from a claimant regarding the installation of non-technical cookies without consent on the website of the sanctioned company.

The respondent argued that the problem was due to an omission in the third-party cookie

implementation controls and that corrective measures had been taken to solve it (blocking of embedded videos, updating of the cookies policy, integration of a CMP, strengthening of audits, etc.). However, the AEPD detected several problems in the behavior of cookies on the website: (i) the cookie management panel presented the options pre-marked as "ON", which is not admissible; (ii) even after rejecting unnecessary cookies, the website continued to install segmentation and performance cookies; (iii) there was no accessible and permanent mechanism to modify consent during browsing; and (iv) the information on cookie management was limited to instructions for the browser, which is not sufficient as a sole mechanism.

In conclusion, the AEPD considered that there was an infringement of article 22.2 of the LSSI based on the installation of non-technical or necessary cookies without prior consent, the installation of non-technical cookies even after express refusal, and the absence of a mechanism to modify or withdraw consent at any time. Thus, a fine of 10,000 euros was imposed for a minor infringement of article 22.2 of the LSSI, aggravated by recidivism, as the entity has already been sanctioned for similar facts in 2023.

# 3. Judgments

## The CJEU supports the determination of penalties under the GDPR based on the concept of 'undertaking' as used in competition law

On February 13, 2025 the Court of Justice of the European Union (CJEU) published itsjudgment in case C-383/23, in which it ruled on a question referred for a preliminary ruling by the Court of Appeal of the Western Region of Denmark. This was in response to the appeal filed by a Danish chain of furniture stores against the amount of an administrative fine imposed on it for failing to retain personal data for the requisite period.

Initially, the chain in question was fined €200,000 for breaching article 5.1.e) of the GDPR, such amount being calculated based on the volume of business of the corporate group to which it belonged. In analyzing that volume in order to calculate the fine, the Danish authorities took the view that the concept of an undertaking to be considered should be the concept according to competition law, whereby an undertaking is looked upon as an "economic unit".

The CJEU's response was based on article 83 of the GDPR, which stipulates that fines must be proportionate and dissuasive. It also drew a distinction between the calculation of the maximum amount of the fine and the proportionality of the fine. The Court nevertheless affirmed that the term “undertaking” must be understood in accordance with articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU), i.e. as an economic unit, within the meaning of competition law.

## The CJEU rules on the extent of the data subject's right of access and the logic employed in the adoption of automated decisions

An Austrian telecommunications company refused to extend a contract with a customer based on an automated assessment of her creditworthiness, according to which the customer’s credit rating was not sufficient for the formalization of the contract. The customer took the matter to the Austrian data protection authority, which ordered the company to provide meaningful information regarding the logic on which the automated decision was based.

The company appealed the order, claiming that it was not required to disclose further information due to trade secrets, and the relevant Austrian court found that the company had breached the GDPR by failing to provide sufficient information regarding the logic behind the automated process. However, the application for enforcement of this decision was rejected by the enforcement authority

in Vienna, which took the view that the company had complied sufficiently with its obligation to provide information.

The customer appealed to the referring court, which referred questions to the CJEU for a preliminary ruling. These questions focused on the interpretation of article 15.1 h) of the GDPR, which stipulates that the data subject has the right to obtain meaningful information on the logic involved in automated decisions, including profiling.

In its decision on case C-203/22, the Court of Justice clarified that, in the case of automated decisions, the data controller must explain in a concise, transparent, intelligible and easily accessible manner the procedure and principles applied when using the data subject's personal data. In addition, if the information includes protected third-party data or trade secrets, the controller must communicate such information to the competent supervisory authority or court, which must balance the rights and interests at issue with a view to determining the extent of the data subject's right of access.

## The CJEU recognizes the right to rectification of data regarding a person's gender without proof of gender reassignment surgery being required

Following a question referred for a preliminary ruling by a Hungarian court, the CJEU examined the case of a person who requested that their name and gender be corrected in the Hungarian national asylum register, presenting medical certificates which confirmed their male gender identity. The administration nevertheless rejected the request due to the absence of proof that sex change surgery had taken place.

In its decision on this case (C-247/23), the CJEU ruled that, by virtue of article 16 of the GDPR, a person has the right to rectify personal data relating to their gender without needing to prove that they have undergone reassignment surgery, and that medical certificates proving their identity are sufficient, based on the principle of data accuracy. It adds that a Member State cannot make the exercise of the right to rectification dependent on the existence of a national gender recognition procedure or require surgery, as that would breach the rights to integrity and to a private life enshrined in the EU Charter of Fundamental Rights.

## The CJEU's Advocate General issues an opinion on case C-654/23 concerning the relationship between the GDPR and the ePrivacy Directive

In the opinion delivered within the framework of case C-654/23, Inteligo Media SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Carácter Personal (ANSPDCP), in response to the request for a preliminary ruling made by the High Court of Bucharest, Advocate General Szpunar, in his conclusions, affirmed that the provision of an apparently free service for advertising purposes may constitute a form of direct marketing pursuant to article 13 of the Directive on privacy and electronic communications (Directive 2002/58/EC). The sending of newsletters without prior consent would therefore be lawful provided the requirements of article 13.2 of that directive are met, without the need for recourse to article 6 of the General Data Protection Regulation (GDPR) as an additional legal basis.

The case examined concerned a website that offered limited free access to contents which could be extended by registering with an email address, whereas full access required payment. After registration, the user - without subscribing to the paid plan - received a newsletter with news about the site.

The Advocate General concluded that this newsletter constitutes direct marketing, since the economic model (soft paywall) is designed to induce the user to contract a paid subscription service. The view formed was that the provision of personal data (such as an email address) in exchange for content can be looked upon as the consideration for a service, which falls within the concept of "sale" under article 13.2. This rule is comprehensive in nature, and recourse to the GDPR is therefore not required. He also stressed that the GDPR and the ePrivacy Directive address different fundamental rights, being compatible and complementary in their application.

## The Supreme Court of Extremadura declares justified the dismissal of a security guard who disclosed personal data in a WhatsApp group

The High Court of Justice of Extremadura has confirmed that the disciplinary dismissal of a security guard at Badajoz Penitentiary Facility based, among other factors, on a serious breach of data protection legislation, was justified. The worker was dismissed after being absent from her station for nine minutes while the alarm system remained deactivated, in breach of the handover protocol. The company gave her 48 hours to present submissions, and the employee responded in writing claiming that her actions were justifiable on health grounds and accusing her superior of workplace harassment.

However, the submissions- which included personal data of colleagues, references to shifts, internal protocols and details of operations at the facility - were later shared by the worker herself in a WhatsApp group called "Grupo Extremadura VS" which had almost 400 members from outside the company. The court concluded that this unauthorized dissemination constituted a very serious breach of her duty of confidentiality and an infringement of personal data protection legislation.

The Labor Chamber of the Court, in its judgment 31/2025 of January 21, 2025, app. 795/2024, dismissed the worker's appeal on the grounds that its factual and legal bases were inadequate. The judgment handed down by the court of first instance was therefore upheld and the dismissal declared to be justified, without the worker being entitled to any severance or back pay.

## The National Appellate Court confirms a fine of 40,000 euros imposed on a finance company for processing without legal grounds the data of a victim of identity theft

The National Appellate Court has confirmed the fine of 40,000 euros imposed by the Spanish Data Protection Agency (AEPD) on a company engaging in the management and recovery of loans, for a very serious breach of data protection legislation. The company processed the personal data of a person who had been a victim of identity theft through the fraudulent contracting of a loan, without there being any legitimate basis to support such processing, in breach of article 6.1.b) of the General Data Protection Regulation (GDPR).

Although the affected party reported the identity theft and requested the deletion of their data in March 2021, the entity did not delete it from the ASNEF delinquency file until almost two months later, yet it continued, in the meantime, to process the data without consent and without there being any legitimizing ground for such action. Panel 1 of the Judicial Review Chamber, in its judgment of February 13, 2025, app. 1005/2022, found that the company had not acted diligently and ruled out the application of the exoneration provided for in article 4.2.a) of the LOPD-gdd, given that the data were not accurate and had not been obtained directly from the affected person.

The court stressed that consent must be unambiguous and that the company remained the data controller even after the loan had been assigned. The appeal filed by the finance company was dismissed and it was ordered to pay procedural costs.

## The National Appellate Court recognizes the right of access to personal data blocked in delinquency files

Panel 1 of Judicial Review Chamber of the National Appellate Court, in its judgment of February 13, 2025, App. 2255/2021, dismissed the appeal filed by an entity which managed a delinquency file against a ruling by the AEPD that recognized a citizen's right to access personal data kept blocked in its systems. Although the data had been cancelled and had remained blocked since March 2019, in January 2021, the affected party requested access to information on their prior inclusion in the file, as well as information regarding the entities that had consulted their data and the reason for the cancellation.

The entity refused to provide part of the information requested, arguing that the blocked data cannot be viewed or processed other than by public authorities in the situations provided for by law. However, the National Appellate Court supported the position adopted by the AEPD, stating that allowing the data subject access to their own blocked data - that processed during the course of the contractual relationship - does not constitute a processing operation pursuant to the GDPR and the LOPD-gdd.

The court stressed that the right of access endures even after the data has been blocked, as long as it has not been physically deleted. This interpretation guarantees that the party affected remains in control of their data and does not breach the principle of limitation of the storage period. The appellant entity was ordered to pay the procedural costs.

## A bank and a file management company are found guilty of unlawful intrusion on a consumer's right to honor

In judgment 259/2024 of December 20, 2024, app. 367/2022, Toledo Appellate Court confirmed the conviction of a bank and a delinquency file management entity for unlawful intrusion on a consumer's right to honor, due to such consumer's improper inclusion in said delinquency file. The court considered it proven that the legal requirements of the data protection legislation in force at the time of the events , — such as a prior payment demand and proper contractual notification of the person's inclusion in credit information systems — had not been met.

The entity managing the file, as data controller, argued that its role was merely technical and that it had followed the creditor's instructions. However, the court, in line with the position adopted by the Supreme Court, affirmed that the controller of the data file must verify the accuracy, relevance and legality of the data before keeping it, and cannot simply assume a passive role. This lack of diligence constituted a breach of the applicable legislation and an infringement of the fundamental right to data protection.

The two entities were ordered, on a joint and several basis, to pay 10,000 euros for non-pecuniary damages, in addition to which the entity managing the file was ordered to cancel the data of the interested party. The judgment stresses the active responsibility of the data controller and the need for rigorous protection of personal data to prevent unlawful intrusion.

## A court in Murcia orders the wiping of delinquency files after granting a debtor exoneration from liability

In the order of May 3, 2024, app. 79/2024, the No. 2 Commercial Court of Murcia granted the debtors an exoneration from payment of the outstanding debt, and, as a direct effect of this, activated the data protection mechanism provided for in article 492 ter of the revised Insolvency Law (TRLC). This rule stipulates that the judicial decision granting the exoneration must include an order addressed to

the affected creditors requiring them to communicate the exoneration to the credit information systems (delinquency files) in which the non-payment or default on the exonerated debts had previously been reported.

The aim of this obligation is the updating of registers, so that negative information cannot be unduly maintained to the detriment of the debtor. This protects the right to accuracy and the updating of personal data, in accordance with article 5.1.d) of the GDPR. Likewise, the debtor has the possibility of obtaining evidence of the decision in order to request directly the updating of their data by these systems, which reinforces their right of access, rectification and cancellation.

This order underscores the relevance of the principle of minimization of processing and the need to ensure that data relating to exonerated debts are not used unlawfully and do not continue to affect the debtor's solvency, thereby helping to ensure that delinquency files are properly cleaned up.

## The CJEU clarifies that the advertising of payment arrangements constitutes a promotional offer which is protected by the E-Commerce Directive

Article 6(c) of Directive 2000/31/EC on Electronic Commerce provides that promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, must be clearly identifiable as such, and the conditions to be met to qualify for them must be easily accessible and be presented clearly and unambiguously.

The dispute (case C-100/24) was between a consumer association and a fashion distribution company specializing in catalog sales, which published an advertising message on its website relating to a specific payment arrangement. Specifically, the advertisement included a message that read “convenient purchase on invoice”. The consumer protection association viewed this as an unfair commercial practice, in particular a misleading omission, because no mention was made in the advertising message of the fact that, to be eligible for this arrangement, it was necessary to undergo an assessment of creditworthiness.

When the case reached the Higher Regional Court of Hamburg, a question was referred for a preliminary ruling, asking whether the advertising of a payment arrangement (in this case, "convenient purchase on invoice"), which has a low monetary value but contributes to the safety and legal interests of the consumer, constitute a promotional offer within the meaning of Article 6(c) of Directive 2000/31/EC on Electronic Commerce.

The court found that a commercial offer must be understood to mean any communication whereby a service provider intends to promote goods or services by providing the recipient with an objective and certain advantage that may influence their behavior in their choice of such goods or services. The form of that advantage, and its relevance, are immaterial; it may be, in particular, a monetary or legal advantage or mere convenience, such as enabling the recipient to gain time.

The CJEU also stressed the importance of a teleological interpretation of the rule, indicating that the objective of the directive is to guarantee a high level of protection for consumers.

Finally, the Court concluded that an advertising message mentioning a specific payment arrangement may indeed be regarded as an advertising offer insofar as it provides the recipient of the message with an objective and certain advantage capable of influencing their conduct when choosing a good or service.

## The Belgian Market Court confirms the penalty imposed on IAB Europe and its position as joint controller in the management of the 'Transparency & Consent Framework'

Following the decision by the CJEU on the questions referred for a preliminary ruling by the Belgian Market Court regarding the validity of IAB Europe's Transparency & Consent Framework (TCF), the Belgian court has issued its judgment. Most significantly, the judgment identifies IAB Europe as joint controller in the creation of the chains of consent which store user preferences in relation to the use of their data in the advertising ecosystem.

In February 2022, the Belgian data protection authority ruled that the aforementioned association, which developed the TCF as a self-regulatory framework for the online advertising market, was a joint controller in relation to both the creation of the chains of consent and the subsequent use made of them, imposing a fine of 250,000 euros.

IAB Europe appealed against the decision to the Belgian Market Court, which referred a series of questions to the CJEU for a preliminary ruling. These were ruled upon in March 2024, declaring that chains of consent contain personal data, and that IAB Europe is joint controller insofar as relates to their creation, but not in relation to the subsequent use of such data by other agents.

Having clarified these issues, the Belgian Market Court has now ruled accordingly, limiting IAB Europe's position as joint controller to certain aspects of the functioning of the TCF, confirming the fine of 250,000 euros initially imposed, and maintaining the need for implementation of an action plan to ensure due compliance with the GDPR.

## The National Appellate Court rules on the multi-million-euro penalty imposed by the AEPD on a bank in 2021

The decision in question imposed penalties for breaches of duties of transparency (2,000,000 euros), as well as for the absence of an adequate legal basis for personal data processing operations carried out by the financial institution (4,000,000 euros).

Following an appeal against the AEPD's decision by the institution in question, the National Appellate Court, in its ruling on the matter, agreed with the AEPD in finding that there had been breaches of the applicable legislation, although it differed as regards the legal treatment corresponding to the practices observed, partially upholding the institution's appeal.

The most significant aspect of this ruling is the fact that the National Appeal Court considers there to be an overlapping of offenses, by virtue of which the breaches of articles 13 and 14 of the GDPR, related to the transparency of the information provided to the interested parties, are to some extent covered by the penalty imposed for the breach of article 6 of the GDPR on legal bases. In this respect, there was found to have been a breach of article 6 of the GDPR which overlapped with a breach of articles 13 and 14 of the GDPR, and a single fine of 2 million euros was imposed.

This was, in the opinion of the National Appellate Court, in view of the fact that, had the data protection information provided by the penalized institution in its privacy policies been complete and in full compliance with the aforementioned articles 13 and 14 of the GDPR, the consent of the interested parties (which provided the applicable legal basis in this case) could have been validly obtained. In other words, the National Appellate Court considered the breach of the duty of transparency to be an essential element which is inherent to the breach of article 6 of the GDPR. In this respect, the original penalty was significantly reduced.

This ruling could have important interpretative implications for the future. This same criterion could be applied to other issues, such as potential overlaps between a failure to apply technical and organizational security measures (article 32 of the GDPR) and the duty of integrity and confidentiality (article 5 of the GDPR), which are breaches for which separate penalties are often imposed in cases involving security incidents. It is therefore important to closely monitor possible changes in the criteria of the AEPD in its forthcoming resolutions.

# 4. News update

## Reforms in the field of personal data protection in Latam and the effects thereof on labor relations

Authors: Ricardo Eckardt, Jairo Jaller, Franco Muschi, Mariana Ubidia, Miguel Ángel Rocha and José Alberto González Rebolledo

In a new environment in which data protection has become more important than any other business need, companies are having to review internal processes and policies, and adopt robust measures to ensure regulatory compliance and safeguard the personal data of their employees, candidates, and collaborators. From selection processes to performance evaluations and labor control mechanisms, the processing of personal data has become a central pillar of people management. In addition to this, the use of AI tools generates a significant level of exposure of personal data – which is often sensitive – and this will, in many cases, require the adoption of policies to guarantee the confidentiality of the information that selection and recruitment departments will start to use.

Regulations in the Latin American region have begun to respond to this reality. Peru, Mexico and Chile have already implemented significant legislative reforms in relation to data protection, while in Colombia the legislation dates back to 2012, although employers and workers have become more aware of the importance and sensitivity of the handling of personal data.

This process of assimilation and updating of legislation– which seeks to bring local legislations into line with international standards – places greater demands on employers and calls for more rigorous oversight by the authorities.

We provide below an up-to-date overview of the main legislative developments and practical considerations concerning the protection of personal data in the labor environment in Peru, Colombia, Mexico and Chile.

### Peru

On November 30, 2024, Supreme Decree No. 016-2024-JUS was published, approving the new Regulations for the Personal Data Protection Law (Law no. 29733), and completely replacing the previous regulations. This legislation came into force on March 30, 2025 and marks a milestone in Peruvian regulation by incorporating international standards and establishing new requirements for the processing of personal data. In the area of employment, it introduces substantial changes that call for a comprehensive review and adaptation of business practices linked to the management of employee data.

Most importantly, the new regulation reinforces key obligations for employers in the processing of workers' data.

It introduces a serious offense (for which penalties of up to approximately USD 70,000.00 can be imposed) consisting of failure to fully inform the worker of the processing of their personal data, in accordance with article 18 of the Law. This requires the review and adaptation of all labor information documents (policies, formats, clauses, etc.).

Similarly, failure to fulfill ARCO (access, rectification, cancellation and objection) rights in a timely manner is defined as a minor infringement, making it necessary to review and reinforce internal procedures for the exercise of rights by workers.

The obligation to designate a personal data officer in certain circumstances is envisaged for the first time. Human Resources should be actively involved in this designation, as it may involve changes to functions, access to data, and working conditions.

Finally, the regulation sets out new security measures, such as the obligation to have an up-to-date security document which is disseminated internally and covers access procedures, the management of privileges and use of platforms, among other questions. Its correct implementation is essential to minimize legal risks, strengthen the culture of compliance and promote workers' trust in the organization.

## Colombia

The protection of personal data has become increasingly important in the business environment, especially in the employment context. Since the introduction of Statutory Law 1581 of 2012 establishing the general regime for the protection of personal data, and its regulatory decrees, organizations have been under the obligation to implement measures that guarantee the privacy, security and correct processing of the personal data of their workers.

In recent years, the Industry and Trade Authority (SIC), as the national authority in this area, has reinforced its role in relation to oversight and penalization, issuing new instructions and decisions that require companies to constantly review their internal policies. Recently, greater effort has been made in the assimilation and absorption of the regulations related to data protection and there has been a consolidation of stricter guidelines on the processing of sensitive data, demonstrated accountability and the management of data bases, which has led to a harsher penalization regime and stricter requirements in the documentation of compliance. Most noteworthy among the regulations and guidelines issued in recent times are the external circulars issued by the Industry and Trade Authority on the processing of personal data. These include External Circular no. 002 of August 21, 2024, which addresses the processing of personal data within artificial intelligence systems, and External Circular no. 003 of August 22 of the same year containing instructions for company directors on the processing of such data.

In the labor context, these provisions imply a significant transformation in the way in which companies manage their workers' data. From obtaining informed consent during selection processes to implementing cybersecurity measures, organizations must ensure that their practices respect workers' rights and are compliant with the principles of legality, purpose, freedom, truthfulness, transparency, access, and restricted circulation.

The authority has sought to issue a constant stream of guidelines and directions aimed at guiding businesses and their collaborators in the proper processing of personal data. These instruments include booklets and technical documents on topics such as the designation of the data protection compliance officer, as well as on activities relevant to organizations, such as video surveillance and its proper management in accordance with current legislation.

This regulatory framework seeks not only to protect the privacy of workers, but also to foster an organizational culture based on trust,

transparency, and regulatory compliance. Thus, the protection of personal data has become a central pillar in modern labor relations in Colombia.

## Mexico

On March 20, 2025, a new Federal Law on the Protection of Personal Data in the Possession of Private Parties was published in the Official Gazette of the Federation. This legislation, which replaces the 2010 rules, introduces clearer and more robust provisions to ensure that the processing of personal data in Mexico is lawful and secure. Below, we explore the main changes and their impact on the Latin American business environment.

Greater clarity and obligations: the new law reinforces ARCO rights (Access, Rectification, Cancellation and Objection), which are now precisely defined and explicitly recognized, eliminating the ambiguity of the previous legislation. In addition, it imposes stricter obligations on companies and individuals who handle personal data, whether on physical or electronic media or in any other form. The requirements include most notably:

1. More detailed privacy notices: companies must provide clear and accessible information on the purposes of data processing, specifying: (i) what data is collected, including sensitive data; (ii) which require express consent and, (iii) how to exercise ARCO rights.

2. Right to object: data subjects may object to their processing if there is a legitimate cause, such as possible damage or harm, or when the automated use of data affects their rights, evaluates personal aspects (work performance, economic situation or health, among others) or generates undesired legal effects.

3. Mandatory confidentiality: organizations must implement controls to guarantee that anyone involved in handling data treats it as strictly confidential.

4. Data protection culture: companies must promote data protection internally, designating, if necessary, a person or department in charge of handling requests related to ARCO rights.

A new institutional approach: one of the most significant changes is the elimination of the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) as the oversight body. Instead, the Anti-Corruption and Good Governance Department will be responsible for supervision, verification and penalization in relation to personal data matters at federal level. The resolutions of this Department may only be challenged by means of a lawsuit for the protection of constitutional rights in specialized courts, which does away with nullity claims at the Federal Administrative Justice Tribunal.

In addition, the penalties and costs associated with the exercise of ARCO rights are to be calculated based on the unit of measurement and update in force, thereby ensuring that the economic base is up to date.

Impact in the labor area: this reform calls for an urgent review of the administrative practices of businesses in Mexico and the region. Employers must: (i) update privacy notices, contracts, and internal regulations to comply with the new law; (ii) implement processes that guarantee transparency in the handling of employees' data and (iii) train their staff in data protection to avoid legal risks.

These changes will not only boost workers' confidence but also position companies as responsible players in an environment in which privacy is a global priority.

## Chile

After seven years of legislative debate, Chile has a new Personal Data Protection and Processing Law (Law 21.719), enacted in December 2024 and which will come into force in December 2026. This law represents a milestone in the alignment of national regulations with international standards, especially the European Union's General Data Protection Regulation (GDPR), establishing a

robust and modern framework for the management of personal data in Chile.

The new legislation is generally applicable, covering all natural persons and legal entities. The main changes it introduces include most notably, the creation of the Personal Data Protection Agency, an autonomous body whose function is to issue instructions, interpret the law, monitor compliance and apply penalties. This institutional element will be key to the correct implementation and supervision of the new rules.

In the labor field, the law recognizes workers as personal data subjects vis-à-vis their employers. This means that they have the following rights over their data: access, rectification, deletion, objection, portability and blocking of data. These rights cannot be waived and must be respected in all employment relationships, reinforcing the obligation already existing pursuant to article 154 ter of the Labor Code, which requires employers to respect the confidentiality of their workers' private data.

The processing of personal data in the labor context may be carried out with the express consent of the employee, although it is also lawful when it is necessary for the performance of the employment contract, compliance with legal obligations or the satisfaction of the employer's legitimate interests, provided that the worker's rights and freedoms are not breached. Special attention should be paid to sensitive data, such as health-related data, which can only be processed subject to strict conditions and with greater safeguards.

For businesses, the entry into force of the law implies the need to review and adapt their internal data processing policies and procedures. It will be essential to implement measures that guarantee compliance with the guiding principles of the law: legality, purpose, proportionality, quality, accountability, security, transparency and confidentiality. In addition, multinational businesses will need to pay particular attention to the new requirements for the international transfer of data, ensuring that destination countries have adequate levels of protection or that sufficient contractual guarantees are in place.

Over the transition period lasting up to December 2026, businesses will need to foresee the adaptation of their systems, train their staff and keep a look out for the regulations and guidelines that will be issued by the future Personal Data Protection Agency, which will provide greater clarity and give practical meaning to the law.

Correct adaptation to the law is of the utmost importance since non-compliance can lead to significant penalties, with fines of up to 20,000 UTM (approximately 1,466,600 euros), a sum that can be tripled in the event of a repeat offense. This underscores the importance of proactive and responsible management of personal data, both to avoid legal risks and to boost the trust of workers and customers in the organization.

In short, the new law marks a turning point in data protection in Chile, requiring companies to make a real commitment to privacy and data security, especially in the workplace. Early preparation and adaptation will be key to responding successfully to this new regulatory scenario.

## Lorenzo Cotino Hueso and Francisco Pérez Bes take office as president and vice president respectively of the AEPD

On March 3, 2025, Lorenzo Cotino Hueso and Francisco Pérez Bes took office as president and vice president, respectively, of the Spanish Data Protection Agency (AEPD), in a ceremony held at the Agency's headquarters, chaired by the Ministry of Presidential Affairs, Justice and Relations with Parliament, Félix Bolaños.

Lorenzo Cotino underscored the challenges that the “digital tsunami” is posing for privacy, particularly in areas such as digital spaces, health and AI and announced the preparation of a strategic plan to address these challenges. Francisco Pérez Bes in turn highlighted the AEPD’s commitment to

proximity to citizens, transparency, agility and innovation, as well as to institutional collaboration.

Minister Bolaños emphasized the importance of the role played by both positions in the context of the growing tensions between technology and data protection and announced that the law for the protection of minors in digital environments would be approved shortly in the second round at the Council of Ministers, thus beginning its passage through Parliament.

Their appointment was formalized in Royal Decrees 142/2025 and 143/2025, respectively. Manuel Olmedo, Rafael Simancas and the former head of the AEPD, Mar España were present at the event, along with representatives from the public and private sector.

## The AEPD participates in a European coordinated action to analyze the application of the right to erasure

On March 5, 2025, the AEPD announced that it would be participating in a European coordinated action focused on the right to erasure (article 17 of the GDPR). This is one of the most frequently exercised rights and the one about which DPAs most frequently receive complaints from individuals. Specifically, the aim is to investigate whether the processes used are accessible, comprehensible and effective for citizens.

This initiative forms part of the European Data Protection Board's program of actions for 2025, and 32 data protection authorities across Europe will be participating. The AEPD will analyze how a sample of controllers in the public and private sector respond to requests for erasure and will identify good practices and possible deficiencies.

The results will be evaluated jointly and may give rise to follow-up supervisory or enforcement actions in each country. In addition, an aggregated report will be prepared which will provide a general overview of compliance in the EEA and the results will be used to encourage better practices and a coherent enforcement of the right to erasure in Europe.

This action reflects the importance the EDPD attaches to ensuring effective protection of fundamental rights in digital environments, particularly in platforms with a high impact on user privacy. It is the EDPB's fourth Coordinated Enforcement Framework Action, which seeks to strengthen cooperation between the authorities. The previous actions focused on the right to access, the use of cloud-based services in the public sector and the role of data protection officers.

## Green light for the draft AI bill in Spain

The Government has approved the Draft AI Governance Law, which seeks to ensure ethical, inclusive and people-focused use of AI. The law will bring the Spanish legal framework into line with the European AI Act, which has been in force since 2024 and is already partially applicable and will be processed via the fast-track procedure. It should be definitively approved by the Council of Ministers as a bill and will be sent to Parliament for approval.

The text establishes, as a salient issue, which authorities will supervise prohibited and high-risk systems according to their scope of application. For prohibited systems, competence is assigned to the AEPD (biometrics and borders), the General Council of the Spanish Judiciary (justice), the Central Electoral Board (democratic processes) and the Spanish Agency for Supervision of Artificial Intelligence (other uses). As far as high-risk systems are concerned, the Bank of Spain (creditworthiness), the Spanish National Securities Market Commission (financial markets) and the insurance regulator (insurance) have been brought on board.

## Cataluña initiates an AI-based pilot scheme to help in the drafting of court judgments

Cataluña has initiated a pioneering project in Spain with the use of AI in courts through AI4JUSTICE, an AI assistant designed to provide support to judges in the drafting of judgments.

The system enables semantical searches of case law and legal grounds to be made, in order to speed up the resolution of repetitive cases, optimizing time and enabling the judges to focus on more complex cases.

Since September 2024, four judges from the Barcelona Appellate Court have been using AI4JUSTICE in cases related to collar clauses and claims related to incidents with flights. The initial results revealed a reduction in the time taken to draft judgments from two hours to just twenty minutes and annual savings are expected to be 12,000 hours and €552,000 for every twenty judges.

## The Government approves the draft Law for the Protection of Minors in the digital environment

This law has been prepared by the Ministries of Youth and Infancy, Justice, Social Rights and Digital Transformation. Numerous public and private bodies, as well as the European Commission have contributed to the draft law, which was presented in June last year.

The draft law includes, among other measures, increasing the minimum age for social media from 14 to 16 for platforms such as Facebook, Instagram or TikTok (with companies having to implement reliable age verification systems), the obligation for mobile devices to include parental control systems by default that are activated during the initial configuration, and the criminalization of the unauthorized creation and dissemination of images or audios manipulated using AI that are sexually explicit or seriously humiliating.

Penalties have also been toughened up for adults who deceive minors online for sexual purposes, and minors are prohibited from accessing random reward mechanisms - known as "loot boxes" - a system that is included in many video games.

## The Information Commissioner's Office (ICO) publishes publishes its guide on anonymization and pseudonymization

The guide underscores the importance of effective anonymization as a process to ensure that personal data cannot be identified, recommending periodic risk evaluations and "motivated intruder" evidence to ensure that data remain anonymous.

For the ICO, whether data is considered anonymous or pseudonymous depends on the context, aligning its approach in this regard with CJEU case law. The CJEU establishes that it is necessary to assess the ability of the party processing the data to identify the individuals, in order to conclude whether they are anonymous or pseudonymous, based on whether, in each specific case, the controller has reasonable means of identifying the person. What might be considered anonymous by one organization might not be for another, in the specific context of re-identification based on pseudonymized data.

The guide also recommends organizations to adopt a global approach to governance when anonymizing or sharing anonymous data, specifically by adopting measures such as carrying out DPIAs to document anonymization decisions, identify risks, adopt mitigation measures, coordinate with other organizations that may process related data affecting identifiability and define supervisory mechanisms and responsibilities.

## The European Union publishes a draft regulation on regulatory technical standards for subcontracting pursuant to the Digital Operational Resilience Act (DORA)

On March 24, the European Commission published a draft regulation setting out the regulatory technical standards for subcontracting pursuant to the DORA Regulation, which includes standards when subcontracting ICT services that support critical or important functions.

The obligations include rules on proportionality, group application, due diligence, risk evaluation, description and conditions for subcontracting, material changes to subcontracting arrangements and termination rights of the financial institutions. It also specifies that financial institutions must be informed of material changes to subcontracting arrangements and that they have the right to oppose or terminate the contract if risk tolerance levels are exceeded or unauthorized subcontracting takes place.

## 23andMe files for bankruptcy following a security incident in 2023

The US company 23andMe, specialized in DNA analysis and consumer genetic testing has filed for bankruptcy after years of financial losses and a major cyberattack which compromised the personal data of millions of users. 23andMe had compiled genetic information on more than fifteen million people.

Following the bankruptcy announcement, 23andMe said it would be looking to sell, which means that the company and with it the genetic information of its fifteen million clients, will probably be available on the market very soon. The company stated that it would not change the way in which it manages or protects its customers' data and declared that data privacy was an important factor in any potential transaction.

However, the New York Attorney General issued recommendations in relation to this matter, giving consumers instructions to delete the genetic data provided to said company and destroy the samples of DNA supplied.

## EDPD publishes a report on the risks involved in large language models and the mitigation measures available

On April 10, the EDPD published a report providing guidance and tools to manage the privacy risks associated with large language model based systems. The methodology helps identify, assess, and mitigate privacy and data protection risks, supporting responsible development.

The guidance supports articles 25 and 32 of the GDPR, offering security and data protection. However, the adoption of the measures is not intended to replace a DPIA as required under Article 35 of the GDPR, but rather to complement it.

## Publication of the European guidelines on processing of personal data through blockchain technologies

The European Data Protection Board has published Guidelines 02/2025, presently in the public consultation phase. The EDPB underscored the complexity and uncertainty of blockchain in relation to the processing of personal data, which poses specific challenges in complying with the GDPR. The Board indicated that it was crucial to assess the risks for the rights and freedoms of data subjects, some of which could be mitigated through technical measures.

Blockchains have certain properties that can make it difficult to meet requirements such as the right to rectification and the right to be forgotten. The guidelines provide a framework for organizations to carefully consider the use of blockchain technology and the responsibilities of the different actors involved.

## The EDPS publishes an opinion on the extension of the adequacy decision for the United Kingdom

In June 2021, the European Commission adopted two adequacy decisions for the United Kingdom, one under the GDPR and the other under Directive 2016/680 on data protection in connection with criminal offenses, allowing the transfer of personal data from the European Economic Area (EEA) to the United Kingdom. Both decisions included a sunset clause and were set to expire on 27 June 2025, unless renewed. On October 23, 2024, the UK government introduced a Data (Use and Access) Bill which proposes to amend certain elements of the UK data protection law.

Since the legislative process was not expected to conclude before Sr ping 2025, the Commission proposed a technical and time-limited extension for a period

of six months, until December 27, 2025 to allow the UK legislative process to conclude and to maintain adequate protection of the data in the meantime. The Commission requested the European Data Protection Supervisor's (EDPB) opinion, which considered the extension reasonable, underscoring that it was exceptional and caused by the need to assess the updated UK legal framework once it had been adopted. The EDPB clarified that the extension did not revisit its previous opinions regarding the adequacy of the United Kingdom - which would be assessed at the end of the legislative process - nor have any impact on its future decisions and that the opinions issued in 2021 (Opinions 14/2021 and 15/2021) remained valid and should be taken into account in future assessments.

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

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

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

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

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

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

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

For further information see here:

**Data Economy, Privacy and Cybersecurity**

GARRIGUES

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

**Follow us on:**