GARRIGUES

Data Economy, Privacy and Cybersecurity Newsletter

December 2024

Contents

1. Data centers as a key part of the digital economy. Challenges and new horizons

A data center is the physical location that stores information and enables cloud services to exist and be created. Although this may seem a simple description it is not at all, if we take into account that the cloud is now the economy itself.

Alejandro Padín Vidal

In this article we look at the importance of these data centers from a dual angle: first as a necessary element of the technology infrastructure of cloud service providers; and secondly, as a potential critical element of the performance of legal guarantee services based on digital certificates, including electronic identification.

Cloud services in the information and data economy

It is no longer news to anyone in 2024 that **information** is the most highly valued asset in the economy we are living in (we have dropped the adjective "digital" because the economy we are living in is or, is essentially, digital). The companies seen to be the top or largest in the world by any standard (gross revenue, profits, number of employees, market capitalization, etc.) built up their value on the basis of managing information and in many cases personal information only. This is how the names "information economy" or "**data economy**" came into use for today's global economy.

In parallel to this reality there is another in the domain of operations, where the use of technology tools at companies, organizations and economic agents has moved and continues to do so from being on premise towards a new use in the form of cloud services.

We therefore have two undeniable realities: the existence of a **highly valuable asset** in the form of **data** and the **unstoppable bursting onto the scene of cloud services** as the number one choice in the selection of technology solutions by economic operators.

Having established this we will now look at the relationship between data as a valuable asset, cloud services and a data center.

Data centers as a key part of cloud services

The name "Cloud services" has been one of the most successful in the history of marketing in the industry. If anyone is offered services "on the cloud" everything appears to be perfect. It creates the feeling that the client for technology services on the cloud has nothing to worry about, because they can continue to benefit from the whole technology service (be it software, a platform, infrastructure, or another) plus all problems disappear: no space or power is needed, no maintenance engineers

are needed, there is no hardware gathering dust, no cooling or electricity is needed, the system no longer crashes, everything seems clean, aseptic, ethereal, light and so on. Furthermore, information no longer takes up space on our systems, it vanishes into thin air as if by magic and we have permanent and continuous access to it, without any risks. And the truth is, with a few tweaks for precision, this is all real, but not because the cloud service is an ethereal service provided from the troposphere. Far from it, a cloud service is provided via a connection on telecommunications networks between our systems and the provider's technology infrastructure. That remote infrastructure is where the systems and information belonging to our business are stored and it is infrastructure built by the cloud services provider or for use by the cloud services provider. All this allows companies to use technology as a service and on demand, which gives it greater flexibility and enables it to channel the costs of using it as operating expenditure instead of as capital expenditure.

Had it not been marketed so successfully, what we now know as a cloud service could perfectly well have been named a basement service, because it involves hosting the technology infrastructure that gives us the service, as well as all the information that is stored and processed in that service, in a basement or a building owned by a third party. But that name would not be quite as appealing.

This shows, therefore, how the data center is a key part in the provision of cloud services and how, as the popularity of these services grows due to the advantages they bring, the need for space and hardware also increases. Whatever type of cloud services are to be provided (public cloud, hybrid, private) or whatever approach is taken for the data center (hyperscale for large providers, collocation for the middle market, edge for specialized services or close proximity and latency), this sector is upward moving with growing opportunities which are taking place under the rules and regulations on the digital economy.

Regulatory angle and value as a key asset for the economy

The data and information economy, or the economy in and from which we live is led by companies which, as we mentioned, built up their value on the direct or indirect management of information and data. Four of the five largest companies in the world by market capitalization in 2024 are digital or tech companies, six of the top ten. A large majority of the hundred largest companies in terms of capitalization are technologically dependent or make intensive use of cloud services.

As we have said, data centers are the infrastructure that stores hardware and key systems for providing cloud services. Bearing in mind that "the cloud" is not a cloud at all but a basement or a building, we can see how it is an essential part of economic flows in cloud services.

Moreover, data centers are always going to tend to be located close to the user, for both technology-related and regulatory reasons. From a technology standpoint, changes in certain solutions create the need for very low latency requirements, which is going to require closer proximity between the source of the data and of processing tools and the user. From a regulatory standpoint, for the European Union in particular, there is legislation that requires data to be kept and processed within the European Union, with very stringent requirements to be able to transfer that data outside the EU. These rules have had a growing effect, because many companies, especially those in critical sectors, require their cloud service providers to have the data stored within the European Union or even within the same country. If, as we have seen, the data center is the element of the cloud services where the data is stored, to meet those requirements it will have to be located in the same country or in the European Union.

This gives rise to other needs in the legal domain, because the location of a data center in a specific area, once we understand its importance, makes that infrastructure subject to the legislation applying

to information security (in the EU, the NIS2 Directive, the DORA Regulation and other cybersecurity directives and regulations) or to data privacy (GDPR and sectoral legislation).

Future of the data center as part of the digital legal guarantee

The explanations given so far paint a clear picture of the value and importance of data centers in the economy, but there is more. We will finish with an idea of what will happen in the future although it is no less appealing and important than that discussed above.

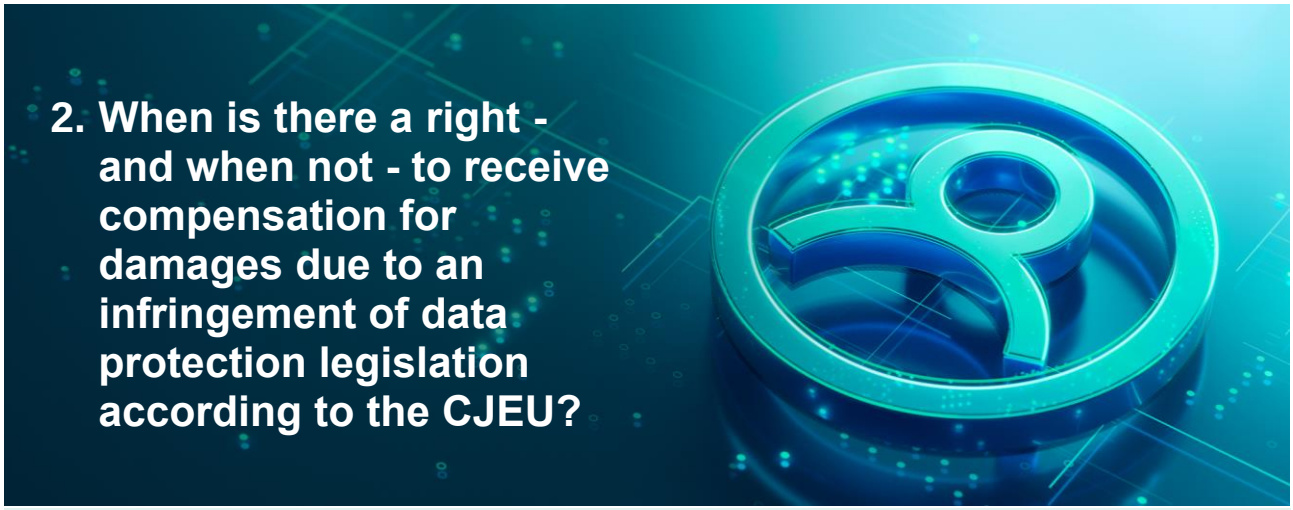
The next station on the journey of the digital economy, of information or data is **digital security** and **digital identification**. As the traditional economy continues to move to, and settle on, the cloud, the necessary legal certainty in that domain needs to be firmly established to be equivalent to the certainty existing in the physical world. A key part is played in this process by identity proofing services using technology based on digital certificates, which in the European Union are regulated in the eIDAS and eIDAS 2 regulations.

These provisions state that identity proofing using qualified electronic certificates or proving digital events and documents using qualified time stamps have the same legal value as the same legal act performed in the physical world. To provide an example that will make this easier to understand, an agreement signed with a qualified digital signature (based on a qualified electronic certificate) has full legal value, and that signature is equivalent to a hand-written signature. It is also presumed to be authentic if challenged by third parties. Similarly, an electronic document (written, graphic, audiovisual, or other type) with an embedded qualified time stamp is enforceable proof with full legal value of the act contained in that electronic document, which is presumed trustworthy.

In this environment, deciding where to add those stamps and, especially, who is to add them is essential, because the participation of a regulated entity is needed, an officially qualified trusted third party who will issue those stamps with fulfillment of all the formalities and requirements laid down by the legislation for that act to have the maximum validity envisaged in the law. In this context, if issuing those stamps is added to the storage of information or the processing of that information at the data center itself, those data centers will become a directly inherent part of digital trust and of legaltech services which are the future of the economy.

This will require the necessary collaboration between regulated trust entities, issuers of qualified electronic certificates, and data center sponsors or managers. To increase the power of that alliance, law specialists need to be added advising on how to provide solutions to digital legal security issues, by adding a legal guarantee layer to the joint technological solution.

This article is designed to prompt reflection by the market with the future in mind and to prompt companies to ensure that they have the technology and legal advice they need to take them to that next station and set in motion the next stage of the route towards technological change on solid and solvent foundations.



2. When is there a right - and when not - to receive compensation for damages due to an infringement of data protection legislation according to the CJEU?

The breach of data protection legislation can lead not just to penalties from the competent authorities, but also to the obligation to compensate the data subjects for the damages sustained. The Court of Justice of the European Union (CJEU) has recently ruled on the subject, creating case law regarding the requirements and limits of civil liability in this area. In this article we will analyze the criteria offered to date by the CJEU.

Cecilia Rosende, Ana López**, Alberto Pimenta** and **Antonio Entrena**

Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), established the right of individuals who had suffered material or non-material damage as a result of an infringement of the Regulation to receive compensation for that damage (article 82).

It also contemplated the possibility of joint protection from these types of breaches, whereby data subjects may authorize certain non-profit bodies, organizations or associations to lodge a complaint on their behalf (article 80).

In this context, doubts have arisen regarding the scenarios in which such right to compensation exists, which has led to various referrals for a preliminary ruling from the CJEU, to date with respect to individual legal actions.

The referrals made by the national courts to the CJEU have been diverse, ranging from whether the existence of a breach of personal data legislation gives rise, in all cases, to a right to compensation, to the rules on liability that are applicable in such event and including, the grounds for relief, among others.

These doubts have arisen in a wide variety of cases such as: **the processing of data related to political affinities without the data subject's consent** (judgment of May 4, 2023, **case C-300/21**, *Österreichische Post AG*); **claim in the case of a cyberattack and the publication of personal data on the internet as a result of that attack** (judgment of December 14, 2023, case **C-340/21***Natsionalna agentsia za prihodite*); **disclosure of personal data without consent on the website of a municipal council, specifically of the agenda of a meeting of the municipal council which referred to a judgment** (here too the judgment was handed down on December 14, 2023, case **C-456/22**, *Gemeinde Ummendorf*); **the processing by an employer of the health data**

of an employee (judgment of December 21, 2023, case **C-667/21**, *Medizinischer Dienst der Krankenversicherung Nordrhein*); **the handing over to an unauthorized third party by mistake of documents concerning a purchase, containing personal data including the customer's income and bank details** (judgment of January 25, 2024, case **C-687/21**, *MediaMarktSaturn*); **receipt of commercial communications by the data subject despite having objected** (judgment of April 11, 2024, case **C-741/21**, *juris GmbH*)**; disclosure to third parties, by mistake, of the tax return of the data subjects** (judgment of June 20, 2024, case **C-590/22**, *PS*); **theft by third parties of the personal data stored on a trading application** (judgment of June 20, 2024, **C-182/22 and C-189/22**, *Scalable Capital*); **dissemination of video footage featuring a character that imitated the applicant, a well-known journalist, without his consent** (judgment also of October 4, 2024, case **C-507/23**, *Patērētāju tiesību aizsardzības centrs*); or **the publication of personal data not legally required on the commercial register of a Member State** (judgment also of October 4, 2024, case **C-200/23**, *Agentsia po vpisvaniyata*).

Although questions will continue to be referred for a preliminary ruling, the criteria set out below can be drawn from the judgments handed down to date by the CJEU.

Criteria of the CJUE

1. There is no "automatic right to compensation" due to the infringement of data protection legislation

The **mere existence of a breach of** data protection legislation does not **automatically generate the right to compensation**. The following **three requirements** must be cumulatively met: i) the existence of an **infringement** of the provisions of the GDPR; ii) the data subject must have sustained **damage**; and iii) there must be a **causal link** between the damage and the infringement.

This was clearly established for the first time by the judgment of May 4, 2023, case C-300/21, *Österreichische Post AG* (paragraphs 32 – 36 and 42) and this has continued consistently in subsequent rulings (judgments of December 14, 2023, case C-340/21 *Natsionalna agentsia za prihodite*, paragraph 77; also of December 14, 2023, case C-456/22, *Gemeinde Ummendorf*, paragraph 14; of December 21, 2023, case C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, paragraph 82; of January 25, 2024, case C-687/21, *MediaMarktSaturn*, paragraph 58; of April 11, 2024, case C-741/21, *juris GmbH*, paragraph 34; of June 20, 2024, case C-590/22, *PS*, paragraphs 22 and 24-25; also of June 20, 2024, C-182/22 and C-189/22, *Scalable Capital*, paragraph 41-42 y 57; of October 4, 2024, case C-507/23, *Patērētāju tiesību aizsardzības centrs,* paragraph 24 and 26-27) also of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraph 140 and 159).

2. Whereas the concept of compensation for damages is governed by EU law, the amount of the damages is decided by the legislation of each Member State

To the extent that there is no express reference to the law of the Member States, the concept "**material or non-material damage**" and the right to "**compensation for the damage suffered**" set forth in article 82 of the GDPR must be **interpreted autonomously**. That is, the interpretation must follow EU law and must be interpreted uniformly in all the EU Member States and does not need to coincide with the interpretation that may be made in relation to these concepts under the national law of each Member State (judgments of May 4, 2023, case C-300/21, *Österreichische Post AG*, paragraphs 29-30 and 44 and October 4,2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraph 139).

However, to the extent that the GDPR does not contain any provisions in this regard, the **determination** or **quantification of the compensation will be governed by the national law of each Member State**, respecting, in all cases, the principles of equivalence and effectiveness (judgments of May 4, 2023, case C-300/21, *Österreichische Post AG*, paragraphs 54 and 59; of December 21, 2023, case C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, paragraphs 83 and 101; of January 25, 2024, case C-687/21, *MediaMarktSaturn*, paragraph 53; of April 11, 2024, case C-741/21, *juris GmbH*, paragraphs 58 and 63; of June 20, 2024, case C-590/22, *PS*, paragraph 40; also of June 20, 2024, C-182/22 and C-189/22, *Scalable Capital*, paragraphs 27 and 33; of October 4, 2024, case C-507/23, *Patērētāju tiesību aizsardzības centrs,* paragraph 32, also of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraph 152).

Specifically, as the most authorized academic opinion has underscored, in cross-borders scenarios, the rules on conflicts in each Member State will determine the national legislation applicable, since Regulation (EC) no, 864/2007 on the law applicable to non-contractual obligations (Rome II) excludes from its scope, non-contractual obligations arising out of violations of privacy deriving from rights relating to personality (article 1.2 g) of the Rome II Regulation). In Spain, the rule on conflict applicable will be article 10.9 of the Civil Code (which provides that "non-contractual obligations shall be governed by the law of the place where the event from which they arise occurred").

In addition, according to article 79.2 of the GDPR, both the courts of the Member State where the controller or processor has an establishment, as well as the courts of the Member State where the data subject has his or her habitual residence (unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers) will have jurisdiction. The dual nature of the jurisdiction applicable (apart from possibly applying the forums envisaged in Regulation (EU) no. 1215/2012 of the European Parliament and of the Council, in accordance with Whereas 147 of the GDPR) could lead to situations of forum shopping, that is of choosing the courts in the most favorable jurisdiction.

3. Extent of the compensation

a. Material or non-material damage

The data subject is entitled to compensation **both for the material and non-material damage suffered** (such as moral damages for example), **without requiring** a **specific threshold of seriousness** (judgments of May 4, 2023, case C-300/21, *Österreichische Post AG* -paragraphs 45 – 51-; of December 14, 2023, case C-340/21 *Natsionalna agentsia za prihodite* paragraph 78; of January 25, 2024, case C-687/21, *MediaMarktSaturn*, paragraphs 59 and 60; of April 11, 2024, case C-741/21, *juris GmbH*, paragraphs 36 and 41; of June 20, 2024, case C-590/22, *PS*, paragraph 26; also of June 20, 2024, C-182/22 and C-189/22, *Scalable Capital*, paragraph 44; and of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraph 149).

The GDPR itself (Whereas 85) underscores that "a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

In order for the damage to confer a right to compensation, it is necessary to **evidence** its **existence and negative consequences** (judgments of January 25, 2024, case C-687/21, *MediaMarktSaturn*, paragraphs 60 and 61; of June 20, 2024, case C-590/22, *PS*,

paragraphs 34 and 35; and of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraph 141-142).

A **data subject's fear of the potential misuse** of their personal data by third parties in the future following an infringement, **could constitute non-material damage eligible for compensation**, although it is necessary to evidence that such fear is **well founded** (judgments of December 14, 2023, case C-340/21 *Natsionalna agentsia za prihodite*, paragraphs 83-85; of June 20, 2024, case C-590/22, *PS*, paragraph 32; and of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraphs 143-144).

Similarly, a **loss of control over the personal data for a brief period of time** could cause the data subject "non-material damage" which give rise to a **right to compensation, if** the data subject can prove that they have **actually suffered such damage, however slight** (judgments of January 25, 2024, case C-687/21, *MediaMarktSaturn*, paragraph 66; of June 20, 2024, case C-590/22, *PS*, paragraph 33; or of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraph 150).

As indicated previously, a mere infringement of data protection legislation does not grant data subjects the right *per se*, to require compensation from the infringer. They must **evidence** that **they have actually suffered the damage claimed, however minimal** (judgment of December 14, 2023, case C-456/22, *Gemeinde Ummendorf*, paragraph 22). However, **a purely hypothetical risk of misuse by an unauthorized third party cannot give rise to compensation** if, for example, it is demonstrated that **no third party became aware of the personal data at issue** (judgment of January 25, 2024, case C-687/21, *MediaMarktSaturn*, paragraph 68).

Finally, the CJEU has established that, **where the damage suffered by the data subject is not serious, a national court may compensate for it by awarding minimal compensation to the data subject,** provided that such minimal compensation compensates in full the damage suffered (judgments of June 20, 2024, C-182/22 and C-189/22, *Scalable Capital*, paragraphs 45-46 and October 4, 2024, case C-507/23, *Patērētāju tiesību aizsardzības centrs,* paragraph 35). Even giving an apology may constitute a standalone or supplementary form of redress of a moral damage, in accordance with the national law applicable. In particular, where it is impossible to restore the situation existing before the damage was caused and provided that this form of redress compensates in full the damage suffered by the data subject (judgment of October 4, 2024, case C-507/23, *Patērētāju thiesību aizsardzības centrs,* paragraphs 36 and 37).

b. **Compensatory, not punitive function**

The right to compensation under article 82 of the GDPR, must fulfill a **compensatory function**, whereby the financial compensation must fully compensate the damage suffered as a result of the infringement. However, compensation for **punitive damage** may **not** be imposed pursuant to the GDPR (judgment of May 4, 2023, case C-300/21, *Österreichische Post AG*, paragraphs 57 and 58; of December 21, 2023, case C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, paragraphs 84 and 102; of January 25, 2024, case C-687/21, *MediaMarktSaturn*, paragraph 47; of April 11, 2024, case C-741/21, *juris GmbH*, paragraphs 60 and 61; of June 20, 2024, case C-590/22, *PS*, paragraphs 41-42; of October 4, 2024, case C-507/23, *Patērētāju tiesību aizsardzības centrs,* paragraph 34 or also of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraph 153).

To the extent that the imposition of administrative fines on the one hand and the determination of compensation on the other reflect different regulatory areas, the criteria of the former, cannot be used to assess the amount of the latter (judgments of April 11, 2024, case C-741/21, *juris*

GmbH, paragraph 57; of December 21, 2023, case C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, paragraphs 85 and 86, of June 20, 2024, case C-590/22, *PS*, paragraph 43; also of June 20, 2024, C-182/22 and C-189/22, *Scalable Capital*, paragraphs 22, 39 and 44; or of October 4, 2024, case C-507/23, *Patērētāju tiesību aizsardzības centrs,* paragraphs 39 to 41).

Given the exclusively compensatory function of compensation, elements such as the degree of seriousness of the damage or the potentially intentional nature of the infringement by the data controller should not be taken into account for the purposes of compensation for damage and only the damage suffered by the data subject must be borne in mind (judgments of April 11, 2024, case C-741/21, *juris GmbH*, paragraph 64; of June 20, 2024, C-182/22 and C-189/22, *Scalable Capital*, paragraphs 28-30; or of October 4, 2024, case C-507/23, *Patērētāju tiesību aizsardzības centrs,* paragraph 42-43). Indeed, it cannot be held as a matter of principle, that physical injury is, by its nature, more serious than non-material damage (judgments of June 20, 2024, C-182/22 and C-189/22, *Scalable Capital*, paragraphs 38 and 39 or of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraph 151).

In turn, the controller's attitude and motivation cannot be taken into account in order to award redress that is "smaller" than the damage suffered by the data subject (judgment of October 4, 2024, case C-507/23, *Patērētāju tiesību aizsardzības centrs,* paragraphs 44-45).

c. **Fault-based liability with a reversal of the burden of proof**

The **data subject** must evidence the **existence of the infringement and of** the **damage suffered**, whereas it is the **data controller** that must prove the **absence of fault in the event** giving rise to the damage if it is to be exempt from liability, because the existence of fault is presumed to exist (judgments of December 21, 2023, case C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, paragraphs 93-94, 98-99 and 103; of April 11, 2024, case C-741/21, *juris GmbH*, paragraphs 46 and 47; of June 20, 2024, C-182/22 and C-189/22, *Scalable Capital* paragraph 28; or of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraph 154 and paragraphs 160-164) or the **absence of a causal link** between the potential data protection infringement and the damage suffered by the data subject (judgment of December 14, 2023, *Natsionalnaagentsia za prihodite*, C-340/21, paragraph 70 and 72).

Thus, where the personal data breach has been committed by **cybercriminals**, the **data controller** may be **exempt** from liability, **if it proves that it did not breach the data protection obligations** to which it is subject (judgment of December 14, 2023, *Natsionalnaagentsia za prihodite*, C-340/21, paragraph 70-72).

However, the controller **cannot avoid liability** by relying on **negligence or failure on the part of a person acting under its authority**, to the extent that it is up to the controller to ensure that its employees apply its instructions correctly (judgment of April 11, 2024, case C-741/21, *juris GmbH*, paragraphs 49 and 52). In addition, **the existence of a non-binding advisory opinion** issued by a supervisory authority to the controller does not exempt the controller from liability either (judgment of October 4, 2024, case C-200/23, *Agentsia po vpisvaniyata*, paragraphs 174 - 176).

Conclusion

It is not uncommon for data subjects that have sustained a personal data breach to seek to determine the civil liability of the party that has committed the breach in question.

But it is essential to bear in mind the boundaries of liability marked by the CJEU, because the mere existence of a personal data breach does not automatically determine the award of compensation. Indeed, such compensation is only received where the data subjects have actually suffered damage and there is a causal link with that damage, which must be evidenced, however slight. In addition, compensation must compensate for the damage suffered but may not be punitive or a deterrent.

3. Data protection authorities' decisions

A hospital chain is fined €200,000 for infringing article 32 GDPR, in relation to the maintenance of a piece of software for managing electronic medical records and invoicing

Decision PS-00351-2023 of September 30, 2024 arose from a complaint against a hospital chain filed with AEPD, the Spanish data protection agency, by reason of security shortfalls in maintenance of the software used at all its clinics for the management of medical records and invoicing.

As part of the proceeding, AEPD initiated preliminary investigations to examine the data processing agreement between the hospital and the software provider, the risk and impact assessments performed, as well as the security measures in place.

The AEPD identified a number of shortfalls in the hospital's security measures, including a lack of traceability in access control, a failure to conduct specific audits of the software and an insufficient data encryption system.

Although the hospital put in place several corrective measures during the proceeding - such as enhancing the encryption system and restricting the number of users with administration permissions -, the AEPD concluded that it had not implemented adequate security measures, such as a robust encryption system and regular audits, which amounts to an infringement of article 32 GDPR. Additionally, the AEPD noted that due to having entered into contracts with the public sector for the provision of healthcare services since 2022, the hospital is required to comply with the Spanish National Security System (ENS), but it had not fulfilled the requirements laid down by that system either.

Accordingly**,** the hospital was fined €200,000 for infringement of article 32 GDPR, as defined in article 83.4 GDPR, taking into account the negligence on the hospital's part by not putting in place adequate security measures, the connection of its activity with the large scale processing of personal data (including special categories of data) and the absence of specific audits on the software used.

AEPD imposes a fine for infringement of article 6.1 GDPR by disclosing and including private phone numbers of local police officers in a local council's emergency plan

This penalty proceeding was initiated in connection with two complaints filed with the AEPD by the Municipal Police Union and a private individual, in which they reported a potential data protection violation by a local council, due to having included and disclosed without authorization the mobile phone numbers of public servants in the police force in emergency plans drawn up by a consultancy firm.

During the performance of fire drills in January 2023 at the municipal police headquarters for a certain district, police staff used an "Emergency Plan" document containing a directory with personal data and private phone numbers of members of the police force. This data had not been provided or authorized for these purposes by the police officers concerned, and the General Directorate for the Municipal Police had provided them to the consultancy firm without the data subjects' knowledge or consent. It was found, moreover, that at other police units landline numbers were used instead of private mobile phones, and that a few employees listed on the directory were retired, had moved to another division or were on sick leave.

In decision PS-00374-2023 of October 4, 2024, the AEPD determined that the processing of the police officers' personal data, namely their private mobile phone numbers, did not meet any of the conditions for lawful processing contained in article 6.1 GDPR. The data subjects' consent was not obtained nor was it evidenced that the processing is necessary for compliance with a legal obligation, the performance of a contract, the protection of vital interests, the performance of a task carried out in the public interest or for the purposes of legitimate interests.

The local council argued that the inclusion of those numbers was necessary for emergency coordination, under Law 17/2015 of the National Civil Protection System and Royal Decree 393/2007. The AEPD concluded, however, that no legislation specifically required the use of private mobile phones and that landline numbers were used in other emergency plans.

Both the local council and the consultancy firm deleted the personal data from the emergency plans after being informed of the infringement, in a remedial action that was assessed positively by the AEPD. The AEPD issued a decision determining that the local council had infringed article 6.1 GDPR, defined as a very serious infringement in article 83.5.a) GDPR and article 72.1.b) of the Spanish Data Protection Law (LOPDGDD). The decision declared the existence of an infringement and ordered it to be notified to the Ombudsman, but no additional measures were imposed due to the deletion of the personal data already performed by the local council and the consultancy firm.

AEPD levies a €50,000 fine for not protecting workers' data correctly in a mediation process related to workplace harassment

The claimant, a worker at a well-known occupational health and security company, filed a claim with the labor and social security inspection authority in respect of a potential case of workplace harassment. The employer disclosed in its final mediation report to the inspectors all the personal data of the claimant in addition to those of the respondents also.

In its decision PS-00012024, the AEPD held that the integrity and confidentiality of processing under article 5.1 f) (integrity and confidentiality principle) and article 32 (security of processing) of the GDPR had been infringed.

The AEPD concluded therefore that the employer had not fulfilled its owed duty of care and there had also been a number of aggravating factors such as the nature and scope, the intentional or negligent character, the category of the data, and the connection of the infringer's activity with the processing of personal data. It imposed a €30,000 fine for infringement of article 5.1 f) GDPR and another €20,000 fine for infringement of article 32 GDPR. Furthermore, in the AEPD's opinion, the employer had not evidenced the security measures that it has in place to ensure that no documents they draw up contain personal data that has not been de-identified.

Disclosing personal data without a lawful basis can carry a €100,000 fine

In decision PS-00245-2024, the AEPD imposed a fine on an electricity retailer after finding that certain items of data of the

individual filing the claim had been disclosed directly to an electricity company for the drawing up of a supply contract, where the claimant had never communicated or had any relationship with that electricity company.

The retailer explained in its reply to the AEPD that, in the process of sending the contract to the claimant, an error had arisen by the person who handled the petition, which caused a mix-up over the two entities to which the operator provided services.

In this case, the AEPD held that it had been evidenced that the respondent had violated article 6.1 GDPR, because it processed the claimant's personal data without having a lawful basis. Although the respondent stated that the facts arose as a result of an error by the sales individual, that does not detract from the fact that the illegal processing took place, nor does it make up for the absence of a lawful basis when processing the data, and it determined a €100,000 fine for infringement of article 83.5 a) GDPR.

AEPD imposes a €300,000 fine on a bank for accessing personal data contained in a solvency file without having a contractual relationship with the data subject

The claimant had entered into a mortgage loan with the bank, and his failure to keep up the payments gave rise to a court proceeding for a monetary claim which was settled out of court by entering into a settlement agreement. After signing the agreement, the claimant learned that the financial institution had accessed his personal data contained in a solvency file up to 47 times after the date of that agreement.

In decision PS-00380-3034 of October 22, the AEPD held that article 20.1.e) of the Spanish Data Protection Law contains a presumption of unlawful processing of an individual's personal data where they are consulted in the database for the solvency file by anyone having a contractual relationship with the data subject which implies the payment of a sum, or the data subject had requested the conclusion of a contract involving financing, deferred payment or periodic invoicing. In this case, however, the consultation of the claimant's personal data was done after the contractual relationship had ended, and therefore the bank did not have a legal basis for that access.

As a result, the AEPD levied a €300,000 fine on the bank for violation of article 6.1 GDPR.

AEPD levies a €30,000 fine for each website of a repeat infringer breaching cookie requirements

In decision PS-00524-2023, the AEPD decided a penalty proceeding against an entity providing information society services and owning a number of websites for an infringement of article 22.2 of Law 34/2022 on information society services and e-commerce in relation to the use of cookies and the information included in each cookie policy. The AEPD identified a number of shortfalls, such as the use of its own and third parties' cookies, even though the user had not accepted their use, or the absence of information on installed third party cookies when the user started browsing the website.

This same entity had already been fined by the AEPD, among other violations, for an infringement of article 22.2 of the Information Society Services Law, in an amount of €5,000 for each website. In this case, after holding the repeat infringement of the same nature to be an aggravating factor, the AEPD levied a €30,000 fine on the company for each website (€90,000 in total).

Irish data protection authority (DPC) fines LinkedIn €310,000,000 for engaging in behavioral analysis and targeted advertising without a legal basis

Following a claim by a French non-profit organization, the DPC issued a decision on the processing by LinkedIn of personal data of users of this social media platform for the purposes of behavioral analysis and targeted

advertising without an appropriate legal basis (see the press release). The DPC determined that it cannot be based on (i) consent, because the consent obtained was not freely given, sufficiently informed or specific, or unambiguous; (ii) legitimate interest, as LinkedIn's interests were overridden by those of the data subjects; or (iii) contractual necessity, because the processing was not necessary for performance of the contract. The DPC determined that LinkedIn infringed article 6 GDPR, as well as the lawfulness, fairness and transparency principle set out in article 5.1(a) GDPR. Moreover, the DPC held that the company had not complied with its duty to provide users with the appropriate information (articles 13 and 14 GDPR).

For the described infringements, the DPC levied fines totaling €310,000,000 on LinkedIn.

Italian data protection authority, Garante, fines a software company €900,000 for not adapting its security measures and facilitating a cyberattack

In issue 528 of its newsletter published on October 22, Garante mentions a decision adopted in July against a software company for having ignored for a year recommendations to update security measures made by a software provider and by the National Cybersecurity Agency. Failure to adopt those measures facilitated a ransomware attack which resulted in the extraction of, including the restriction of access to, files containing personal data of approximately 25,000 data subjects, including employees, former employees, candidates and representatives of companies with which the entity carries on business dealings.

The data was published on the dark web and contained identification, contact, access, payment, and criminal record particulars and special categories of data such as information on health and trade union membership.

On top of a €900,000 fine, the company was ordered to analyze the vulnerabilities of its systems, and reduce and identify appropriate risk detection and response times.

A company has been fined for sending more than 200 advertising text messages to a private individual without their consent

On December 3, 2021, a private individual filed a complaint with the AEPD due to receiving unsolicited advertising communications on clairvoyant services. The complaint was based on three grounds: constant receipt of calls and advertising messages, absence of options to cancel subscription and ineffectiveness of being included on the Robinson List.

The AEPD found that the respondent had sent 242 text messages to the complainant over three months, in which it had not included a straightforward free mechanism to object to the processing thereby contravening article 21 of the Information Society Services Law. Despite the complainant's attempts to unsubscribe the messages kept on coming.

The respondent alleged that its activity was not subject to the Information Society Services Law due to not being an e-commerce service and that the text messages were sent in response to a request by the client. It also contended that its operations did not involve the processing of personal data, because they only registered given names and signs of the zodiac. However, the AEPD dismissed these claims and held that the messages were commercial communications subject to the Information Society Services Law.

In a decision dated October 29 under proceeding number: EXP202200418, the AEPD concluded that the seriousness of the infringement was aggravated by their persistence and levied a €30,010 fine on the respondent.

A private individual is fined for installing surveillance cameras capturing images of private areas

On April 17, 2023, a private individual filed a complaint against another for installing a surveillance system at a property that it leased for a horse riding club. The complainant alleged that the cameras captured images of leased areas, such as the training track, the women's bathroom and the parking area, affecting the privacy of clients, including minors and people with disabilities, without their consent or the appropriate information.

The complainant produced proof, in the form of photographs, a notarized certificate and social media posts; and the respondent did not reply to the Agency's request to evidence corrective actions. As a result, in October 2023 a penalty proceeding was initiated for an alleged infringement of article 6.1 GDPR, which requires a lawful basis for the processing of personal data.

In a decision dated October 30 under proceeding number: EXP202305765, the agency held that it had been evidenced that the cameras captured private areas without consent or legal grounds. This amounts to a serious infringement of the GDPR and the Spanish Data Protection Law, which requires video-surveillance to be limited to guaranteeing security without invading third parties' privacy.

The respondent was fined €2,000 and ordered to remove or re-position the cameras within a month to comply with the law.

A political party is fined for using the image of a private individual in its election manifesto without authorization

On May 22, 2023, a private individual filed a complaint with the AEPD against a political party for making unauthorized use of her image in the party's election manifesto. The complainant alleged that, although a photograph had been taken at a public event in April 2023, she had previously specified that she did not want her image to be used for political purposes, which was stated in a WhatsApp message. Despite this warning, the image appeared in the election manifesto and on the party's social media.

The respondent's defense was that the image was of an institutional character and was used as part of the promotion of public activities in the municipality. The AEPD concluded, however, that use of the image in the election manifesto fell outside the original purpose and was not based on the complainant's express consent, as required in the GDPR. The agency held that the original publication of the image by the local council did not authorize its reuse in an election context.

In its decision of October 31 under proceeding number: EXP202308206, the AEPD fined the party €5,000 for infringing article 6.1 GDPR, noting insufficient care in obtaining consent and an unlawful use of personal data.

AEPD levies a €6.5 million fine on a telecommunications distributor for a security breach

In decision ps-00084-2023 the AEPD dismissed the appeal for reconsideration lodged by a telecommunications distributor against an AEPD decision dated December 27, 2023 which fined it €6.5 million in total for an infringement of article 5.1.f) and article 32 GDPR in relation to a security breach involving personal data that occurred in 2021.

The breach caused by Babuk Locker ransomware compromised the confidentiality of certain items of personal data (full names, dates of birth, postal and email addresses) of approximately 13 million clients, former clients, suppliers and employees of the fined company. The AEPD received up to 211 complaints from data subjects involved.

Although the company argued that it had been the victim of a sophisticated cyberattack, the AEPD determined that the security measures implemented by the company were insufficient, in violation of the GDPR. The AEPD also rejected the existence of concurrent infringements of article 5.1.f) and article 32 GDPR, due to considering that the infringement of article 32 takes place

separately from whether a breach of confidentiality ultimately occurred, because the sanction is for the lack or insufficiency of those measures. Whereas the infringement of article 5.1.f) GDPR relates to failure to guarantee an adequate level of security through the appropriate technical and organizational measures, meaning both security and all other kinds of measures.

The respondent filed an application for judicial review with the National Appellate Court requesting a stay of payment as injunctive relief and the confidentiality of certain documents, but the National Appellate Court denied that petition.

AEPD fines a telecommunications company €200,000 for issuing duplicate SIM cards to third parties

In decision ps-00425-2023, the AEPD dismissed an appeal for reconsideration lodged by a telecommunications company against AEPD decision dated May 8, 2024, levying a €200,000 fine for infringement of article 6.1. GDPR, due to an unlawful processing of a data subject's personal data in relation to issuing duplicate SIM cards.

The AEPD held that the company had not acted with the required standard of care by not following the procedure in place for correctly identifying its clients, which gave rise to an unlawful processing of personal data. Although the AEPD agreed with the respondent that the issuing of the duplicate of SIM card is not sufficient by itself to be able to carry out banking transactions in the owner's name, it noted the importance of the standard of care owed by operators to prevent this type of fraud and violations of the GDPR.

Moreover, the AEPD rejected the petition to dismiss the proceeding due to an absence of fault, stating that the company did not take the necessary measures to prevent attempts to change the email address by phone.

A content creator is fined €10,000 for publishing a video of a minor answering questions relating to her sex life

The parents of the minor reported to the police the publication of a video on TikTok and Instagram by a content creator without their consent. That creator, who has thousands of followers on several platforms, alleged that he had asked the minors to inform their parents of the recording and, due to receiving no objections, published the video. However, in decision ps-00471-2023, the AEPD determined that the processing of information relating to the sex life of a minor, due to involving special categories of data, requires specific circumstances as set out in article 9.2 GDPR, in addition to a lawful basis under article 6.1 GDPR. For that reason, the AEPD held that the parents had not given their prior consent as laid down by the requirements in the data protection legislation.

In addition to the infringements of article 9.2 and article 6.1 GDPR, the agency levied further fines for infringements of article 5.1.c) and article 13 GDPR, which added up to €10,000 in total. In relation to the infringement of article 5.1.c) GDPR (data minimization principle), the AEPD noted that the dissemination of the video of the minor on social media is an excessive processing of data, because the news could equally have been given without identifying the minor using the video.

AEPD fines an automotive company €20,000 because its cookies policy is not compliant with the rules

After investigating an automotive company's website of its own initiative, AEPD, in decision ps-00284-2024, initiated a penalty proceeding against that company and levied a €20,000 initial fine for infringement of article 22.2 of the Information Society Services and E-Commerce Law. The agency identified a number of defects in the company's cookies policy, namely: (i) the installing of nontechnical cookies (such as functionality or segmentation cookies) on users' devices when they accessed the website for the first time, after clearing the device's browsing history and

cookies, and without having accepted new cookies or carried out any activity on it; and (ii) that, despite the existence of a mechanism allowing the user to withdraw their consent to the use of cookies after it had been given, nontechnical cookies information continued to be sent to the server it when it should have been deleted.

Lastly, the AEPD issued a decree ending the proceeding due to voluntary payment, because the respondent had paid the fine in an amount of €12,000 making use of the two reductions set out in the initiation decision.

AEPD fines a bank €200,000 for carrying out a processing of personal data without a sufficient lawful basis

The complainant had been a bank employee and after resigning from her job, she kept her corporate mobile phone for her own personal use by signing up to a company program allowing this. Some time after termination of her employment, when she had been using that mobile phone for her own private use, the device showed a message stating that it was being administered remotely by the bank and that she had to enter using her corporate account to continue using it. After contacting the bank, the only solution to make the phone work again was to delete all its contents and restore it to its factory settings. This meant losing the complainant's strictly personal and private information.

On the basis of those facts, the AEPD, as mentioned above, held that the bank carried out a processing of the complainant's personal data without a lawful basis, due to no longer having an employment relationship with her, and there not being any other lawful basis for the processing.

In penalty proceeding EXP202303478, the AEPD fined the bank €200,000 (which was reduced to €120,000 due to voluntary payment) for carrying out a processing of personal data without a sufficient lawful basis under article 6 GDPR.

Three companies fined for their use of Google Analytics cookies

In separate proceedings EXP202315694 (PA/00061/2023), EXP202315693 (PA/00060/2023) and EXP202203580 (PA/00053/2023), the AEPD adopted similar decisions in relation to the use of cookies and similar technology on three companies' websites. The AEPD's analysis focused on the use of Google Analytics cookies by these entities, with the resulting international transfers that this involves.

After analyzing the use of this technology by the companies under investigation, the AEPD held that they were indeed carrying out a processing of personal data in relation to which they acted as controllers. It found further that: (i) it has not been appropriately evidenced that the data subject's personal data had been de-identified before being accessed by Google; and (ii) based on the available documents, Google could have been accessing that information from the U.S., namely, from outside the European Economic Area. Consequently, the use of this technology was involving a transfer of personal data to the U.S.

Therefore, the AEPD ruled that at the time of the facts (before the new framework was established for the transfer of data from the European Economic Area to the U.S., and after the Schrems II judgment declaring the privacy shield invalid), that international transfer had not been legally made under any of the mechanisms set out in the GDPR, and sufficient guarantees had not been provided when they were made. The AEPD therefore held that the investigated entities breached the applicable legislation, as a result of which these three entities were reprimanded.

4. Judgments

The CJEU tackles the lawfulness of the processing of sensitive data by Meta Platforms in the Schrems case

The judgment by the Court of Justice in case C-446/21 | Schrems (Disclosure of data to the general public) arose from the complaint filed by Mr. Maximilian Schrems with the Austrian courts, arguing that an unlawful processing of his personal had been carried out - among others, of data concerning his sexual orientation - by Meta Platforms Ireland on Facebook.

Meta Platforms collects the personal data of Facebook users relating to activities on and off that social media platform (for example, data relating to online platform visits and third parties' websites and apps). Meta Platforms does this through cookies, social plug-ins and pixels embedded in the websites concerned. Moreover, Meta Platforms can also identify the interest that the user may have in sensitive subjects such as sexual orientation, which enables it to it to direct targeted advertising at him.

The question referred to the court concerned whether Mr. Schrems manifestly made sensitive personal data about himself public due to having disclosed the fact that he is homosexual at a panel discussion with public participation, thereby authorizing the processing of that data under the GDPR.

In this context, the Austrian Supreme Court asked the CJEU to interpret the GDPR.

The CJEU replied first that the data minimization principle - provided in the GDPR - precludes all of the personal data obtained by a controller (such as the operator of an online social media platform) from the data subject or third parties and collected either on or outside that platform, from being aggregated, analyzed and processed for the purposes of targeted advertising without restriction as to time and without distinction as to type of data.

Secondly, according to the CJEU, it cannot be ruled out that by making that statement in the panel discussion, Mr. Schrems manifestly made his sexual orientation although it determined that it is a matter for assessment by the Austrian Supreme Court.

The GDPR does not preclude national legislation that allows an infringement of the data protection legislation to be challenged by a competing company

The German Federal Court of Justice, which had to decide a lawsuit between two competing pharmaceutical companies, asked the CJEU to interpret the GDPR. In the judgment in this case (C-21/23 | Lindenapotheke), the CJEU stated that the GDPR does not preclude national legislation that allows competitors of the alleged infringer of the data protection regulations to challenge that infringement before the courts as a prohibited unfair commercial practice. That remedy available to competitors is added to the powers of intervention of the supervisory authorities responsible for supervising and monitoring compliance with the GDPR, as well as the remedies available to data subjects as provided in that regulation.

It held moreover that data concerning health, within the meaning of the GDPR, covers data which a customer provides when ordering pharmacy-only medicinal products online, even if the sale of those products does not require a prescription. Therefore, the seller must inform these customers, in an accurate, comprehensive and easily understandable manner, of the characteristics and specific characteristics of the processing of those data and ask for their explicit consent to that processing.

The CJEU rules on attempts to access personal data stored on a mobile phone

In case C-548/21 | Bezirkshauptmannschaft Landeck, the Austrian police seized a mobile phone in the course of a drug trafficking investigation and tried (unsuccessfully) to access the data on that device without informing the data subject and without the authorization of a court or the Public Prosecutor's Office. The data subject brought an action challenging the seizure with the Austrian courts, which learned in the court proceeding itself about the attempts to gain access by unlocking the phone.

In this context, the Austrian court referred a question to the CJEU as to whether a national legislation that allows the police to act this way is consistent with EU law. In its reply, the CJEU took the view in its judgment that:

a. EU law (the GDPR in this case) does not only apply where the personal data contained on a mobile phone is accessed successfully, but also to attempts to access them.

b. the access to all the data contained on a mobile phone may constitute serious, or even particularly serious, interference, with the data subject's fundamental rights.

c. to avoid an unjustifiable restriction on the investigative powers of the competent authorities, that interference is allowed provided that the national legislature defines with sufficient precision the elements that have to be taken into account for it to be able to take place; in particular, the nature or categories of the offenses concerned.

d. the access must be subject to a prior review performed by a court or by an independent administrative body, except in justified cases of urgency, provided that a fair balance is ensured between the legitimate interests involved.

e. the data subject must be informed of the grounds on which the authorization for the access is based, where that information is not liable to jeopardize the investigations.

The CJEU rules on the disclosure of personal data for promotional purposes in return for remuneration

In case C-621/22, a sports association was fined by the Netherlands data protection authority for having disclosed personal data of its members to two of its sponsors for promotional purposes,

without a legal basis for doing so. The association therefore appealed against the decision to the Netherlands courts claiming that the disclosure of that data was based on a legitimate interest, within the meaning of article 6.1 f) GDPR, consisting partly in creating a strong link between that association and its members and partly in being able to provide added value to their membership in the form of discounts and offers.

In this context, the Netherlands court referred a question for a ruling by the CJEU as to whether the disclosure, in return for remuneration, of personal data of its members to the sponsors of that association for promotional purposes can be justified on the basis of article 6.1 f) GDPR.

In reply to this question, the CJEU did not rule out in its judgment that a commercial interest of the controller, which consists in the disclosure of personal data for promotional purposes, may be regarded as a legitimate interest within the meaning of article 6(1)(f) GDPR, provided that (i) the alleged legitimate interest is lawful and (ii) the controller complies with all its other obligations under the GDPR (with its duty to inform data subjects of the interests pursued, for example). It recalled, further, that recital 47 of the GDPR recital cites, by way of example, direct marketing purposes in general as legitimate interests that may be pursued by a controller.

The CJEU also mentions the other cumulative requirements that must be considered to determine whether that interest has to take precedence over the rights and freedoms of the data subjects, as well as the need to examine whether that interest cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects. On this point, the CJEU suggested that the association could have achieved the alleged interest just as effectively if it had first informed and consulted the data subjects on the disclosure of their personal data to third parties.

Lastly, the CJEU noted that, among the interests to be balanced are the reasonable expectations of the data subject that their data would be disclosed for valuable consideration to sponsors of the association for promotional purposes. In this case, however, the CJEU casts doubt as to whether that expectation may arise.

The Supreme Court confirms the €200,000 fine levied by the AEPD on a telecommunications services company

In judgment number 1569/2024 of October 8, 2024, the Supreme Court dismissed the cassation appeal lodged by a telecommunications services company and confirmed the €200,000 fine levied on it by the AEPD. The fine related to the company's failure to adopt adequate security measures to avoid the fraudulent creation of duplicate SIM cards which enabled unauthorized access to its customers' personal data in contravention of article 5.1.f GDPR.

The respondent company argued that the infringing conduct had to be seen in the light of article 32 GDPR instead of article 5.1.f), because, by being focused on the technical and organizational security measures, it is more precise and therefore must be applied exclusively in cases involving insufficient protection measures.

However, the Supreme Court held that article 5.1 f) GDPR is not simply a general article, because it also imposes a specific obligation to provide adequate security for personal data, including against unauthorized or unlawful processing by adopting appropriate technical or organizational measures. The court underlined that article 5.1.f) does not claim anywhere that it can displace the application of article 32, which instead serves to complement and implement the obligation laid down in article 5.

The Supreme Court allows the AEPD to review in depth the privacy policies of a bank within a penalty proceeding, setting aside an earlier decision by the National Appellate Court

In judgment 1792/2024 of November 11 on appeal 2960/2023, the Supreme Court (panel 3 of judicial review chamber three) upheld the appeal lodged by the AEPD against an earlier national appellate court decision setting aside fines levied by the AEPD on a bank. This proceeding before the AEPD arose from a number of complaints by the bank related to the processing of its personal data for marketing purposes.

Namely, in this case, and upholding the bank's application for judicial review against the AEPD's decision, the National Appellate Court held that the AEPD could not "extend" the subject-matter of the penalty proceeding to include a general review of the bank's privacy policy, because this would mean carrying out a kind of general proceeding against the respondent arising from a limited number of complaints related to a few specific facts. The Supreme Court held, however, that the AEPD did not contravene anywhere the principle forbidding arbitrary decisions or the principle of legal certainty, especially since the reviewed privacy policy was directly related to the examined cases.

In this decision, the Supreme Court has opened the door to allowing the AEPD to review in depth the compliance status of data controllers, especially in relation to their privacy policies as construed broadly, without being categorically constrained by the content of the complaints it has received, and at all times in accordance with the principles and rules governing the penalty proceeding and the actions of the public authorities.

The Supreme Court decides a cassation appeal lodged against Google on balancing the right to protection of personal data and the public disclosure of judgments

The cassation appeal was filed to request the deindexing of certain links on Google's search engine that took users to a judgment by the Supreme Court of Justice of Colombia. The judgment concerned dealt with a family dispute over visitation schedules for a minor. It was argued that the publication of that judgment contravened the right to protection of personal data and affected the appellant's right to reputation, privacy and own image.

In judgment 1775/2024 panel 3 of judicial review chamber three of the Supreme Court dismissed the appeal, based on the argument that the right to protection of personal data is not absolute and must be balanced against other rights at issue, in this case, the duty to publicly disclose courts' judgments. The judgment underlined that the public disclosure of courts' judgments is a legal asset in the public interest, especially in the case of official documents published by a judicial authority carrying out its functions. The court also noted that the information contained in the published judgment did not include data regarded as needing to be de-identified according to the Plenary Decision of the Constitutional Court. It noted, moreover, that sufficient proof had not been provided to evidence that the information was inaccurate or obsolete. For all those reasons, the Supreme Court concluded that the balancing of rights made by the contested judgment was correct and consistent with the law, with the public interest in disclosure of the court judgment taking precedence in this case over the right to protection of personal data.

5. News update

Peru: New Regulations for the Data Protection Law have been published

The new Regulations for the Data Protection Law in Peru, published on November 30, 2024, introduce significant changes to strengthen security and the processing of personal data, to respond to the needs of an increasingly digital environment. Among the new provisions, a new notification procedure within 48 hours has been created for security incidents, the same one involves notifying both the National Data Protection Authority and data subjects. It also introduces the role of Personal Data Officer, an internal position with responsibility for ensuring compliance with the legislation at public and private companies with high data processing levels, especially sensitive data.

The regulations also strengthen citizens' rights by implementing measures such as the portability of data, allowing data subjects to transfer their data among different controllers. Tougher fines have been introduced for infringements of the law, including delays in replying to requests to exercise access, rectification, cancellation and objection rights or the failure to appoint a data officer. These provisions seek to ensure greater transparency and security in the handling of information, they have been adapted to international standards and protect digital rights in a globalized environment.

On the entry into force of these new Regulations, scheduled for March 30, 2025, the previous regulations, in force since 2013, will be repealed.

See here for further information.

The travelers register: Royal Decree 933/2021: challenges and issues

The coming into effect of Royal Decree 933/2021 on December 2, 2024 placed hospitality, car hire and tourism operator businesses under obligation to collect, store and transfer their customers' data to the Spanish authorities. This legislation, which has sparked an intense debate at home and abroad, poses a host of challenges in privacy matters.

This is because in addition to broadening the scope of its obligations to include new actors in the tourism industry, Royal Decree 933/2021 has also significantly increased the amount of personal data that must be collected and transferred to the authorities. All this poses a host of legal doubts and concerns over, among other things, the proportionality and predictability of these obligations. Can companies subject to Royal Decree 933/2021 comply with their obligations without violating travelers' data protection rights? What implications will effective application of this royal decree have for the tourism industry and

how are the obligations it contains aligned with the applicable data protection law? Learn more about the details and issues in this article.

The UN publishes its final report on Governing AI for Humanity

The UN has published its final report on Governing AI for Humanity, determining the need to have a global AI governance system built on a comprehensive and inclusive approach with respect to political, economic and social domains among others.

The report states that existing AI governance initiatives are affected by (i) representation gaps: most governance initiatives are not fully representative; (i) coordination gaps: there is a risk of incompatibility between initiatives from different regions; and (iii) implementation gaps: actions are required to ensure that commitments to good governance translate into tangible outcomes in practice.

To reverse the effects of these gaps, the UN provides seven recommendations that are summarized in the final report and are built around four aims:

The UN ends the report with a call for action to achieve an AI landscape that is inclusive and empowering for every country.

Publication of the provisional version of the EDPB's guidelines for using legitimate interest as a lawful basis

On October 2024, the European Data Protection Board (EDPB) published the provisional version of Guidelines 1/2024 on processing of personal data based on article 6.1.f) GDPR (legitimate interest), which is now at the public consultation stage. These guidelines, updating Opinion 06/2014 of the Article 29 Work Party, contain the main interpretation criteria, CJEU case law and examples to be taken into account when it comes to using that lawful basis.

The guidelines go deeper into the use of legitimate interest for direct marketing purposes, give the cases where a third party's legitimate interest comes into play and explain the meaning of reasonable expectations of the data subject. Any definitive conclusions will have to be based on the final version, however.

Publication of Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)

On October 7, 2024, the EDPB adopted opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s), answering the questions submitted by the Danish data protection authority.

The overall conclusion is that the data controller must always have readily available all the identities of the processors and sub-processors and verify that they all fulfill the security measures laid down by the GDPR.

The extent of that verification depends, however, on the risk associated with the processing concerned. The EDPB also confirms that the controller-processor contract can allow the processor not to follow the controller's instructions if they contradict non-EU legislation, provided that step does not enter into conflict with fulfillment of the GDPR.

The fourth Roundtable of G7 Data Protection Authorities has been held

From October 9 to 11 this year, the 4th edition of the G7 Data Protection Authorities (DPA) Roundtable in Rome was held in Rome, attended by authorities from Canada, France, Germany, Japan, the UK, and the U.S., the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS).

The talks centered around three core subjects: Data Free Flow with Trust (DFFT), the implications of emerging technologies, and

enforcement cooperation, all from the standpoint of the growing use of artificial intelligence (AI).

The key outcomes were a statement highlighting the crucial role of data protection authorities in ensuring that AI technologies are trustworthy and comply with the data protection legislation, a statement on AI and children, and a statement on the importance of having robust mechanisms for international data transfers.

The EDPB launches new guidance on the technical scope of article 5.3 of the ePrivacy Directive

The European Data Protection Board (EDPB) has published new guidelines on the application of article 5.3 of the ePrivacy Directive to new tracking tools, which enlarge upon Opinion 9/2014 of the Article 29 Working Party on device fingerprinting.

These guidelines set out to identify and analyze three key elements for the applicability of Article 5(3) of the directive: (i) information, (ii) terminal equipment and (iii) access or storage. Ambiguities concerning the scope of that provision have raised considerable concerns and therefore need these new guidelines to address the implementation also of what is technically covered by the phase "to store information or to gain access to information stored in the terminal equipment of a subscriber or user".

These new guidelines also address in a non-exhaustive list specific use cases of tracking technology, such as tracking based on IP only or URL tracking.

Has the period for transposing the NIS 2 directive into Spanish law run out before Spain has done so

The NIS2 Directive on measures for a high level of cybersecurity, was formally approved in November 2022, published in the Official Journal (OJ) on December 27, 2022, and came into force on January 16, 2023. Member states had to adopt and publish the necessary measures to comply with the directive before October 17, 2024.

That time period for member states to transpose NIS2 into their internal legislation has run out, however, before Spain has published the definitive legislative framework for its specific adaptation. To date only Belgium, Croatia and Hungary have published their transpositions. Although the directive's recommendations are clear and it is now possible to start the adaptation process to adopt basic cybersecurity measures (such as incident handling, risk analysis and security in the supply chain), the Spanish legislature will have to move to produce a preliminary draft of the provisions as soon as possible to avoid a fine.

The AEPD presents a new methodology for privacy and data protection threat modeling

The AEPD has issued a technical notice to present LIINE4DU 1.0: a new methodology for privacy and data protection threat modeling.

The only privacy threat modeling of this type that has been published and is widely used is LINDDUN (Linking, Identifying, Non-repudiation, Detecting, Data disclosure, Unawareness y Non-compliance).

In the AEPD's view, although LINDDUN is a solid framework for analyzing privacy threats, it has setbacks when used specifically for complying with the GDPR and carrying out an impact assessment relating to data protection. LINDDUN focuses mainly on technical threats, and does not deal to the same extent with the organizational and procedural elements of compliance with the GDPR.

Therefore, the AEPD is working on a new LIINE4DU (Linking, Identifying, Inaccuracy, Non-repudiation, Exclusion, Detecting, Data Breach, Deception, Data Disclosure, Unawareness and Unintervenability) framework focusing on the protection of rights and freedoms and on compliance with the GDPR.

A report has been published on article 36 of Decision 2007/533/JAI on the establishment, operation and use of the second generation Schengen Information System (SIS II)

The Coordinated Supervision Committee has issued a report on the requirements for initiating alerts under article 36 SIS II within the inspection activities of the Schengen Information Systems, due to the increase of this type of alerts in Europe. Remember that the SIS was created to counterbalance the opening up of borders among the Schengen member states, and contains alerts issued by those member states to combat crime and prevent public security threats.

30 data protection supervisory authorities from 19 member states have participated and exchanged impressions for preparation of the report. After identifying differences among the member states, the Committee included a list of the main recommendations for the authorities initiating these alerts, which are to check that (i) all the legal requirements for the alert are fulfilled, (ii) the case and the decision to issue an alert are documented sufficiently by the responsible bodies, (iii) only the data needed to issue the alert is included, and (iv) national procedures have been followed.

Costa Rica: First country to use artificial intelligence to create its country brand strategy

Costa Rica has become the first country in the world to use artificial intelligence to create its country brand strategy, called Essential COSTA RICA. This strategy sets out to plan how the country will be seen in 2035, placing the spotlight on its commitment to the environment and climate change.

To create this strategy Costa Rica worked with Bloom Consulting and gathered information from various sources, including studies on how the country is perceived and documents on sustainability. Using AI, they analyzed this data to gain a better understanding of how Costa Rica is seen and the trends that could influence its image in the future.

Thanks to AI, they were able to identify areas where they can enhance their presence in the world and predict how the media will talk about the country. The strategy's main topics are sustainability and combating climate change, and the idea is to position Costa Rica as a leader in these areas worldwide.

The director of Essential COSTA RICA said that the country is already working on activities with businesses to strengthen their image and promote sustainability.

The EDPB and the European Commission have published their report on the first year of operation of the Data Privacy Framework between the EU and the U.S.

Both the European Commission and the EDPB have assessed in separate reports (one dated October 9 and the other, November 4) whether the Data Privacy Framework between the EU and the U.S. guarantees an adequate level of data protection for EU citizens where their personal data is transferred to the U.S. Both institutions concluded that the U.S. authorities have made an effort and cooperated to put in place the necessary structures and procedures to ensure that the DPF functions effectively along with the various developments that have taken place since its approval.

They highlighted the need for the U.S. authorities to proactively carry out supervision activities to ensure compliance with the principles of the DPF by certified companies. It has also been suggested that additional common guidelines be drawn up between the U.S. and EU authorities on key elements of the DFP, such as specifying the requirements needing to be fulfilled by certified companies.

The European Commission has said that a new periodic review will be carried out in three years to assess progress and the practical application of the new legislation being

produced in the U.S. on privacy and national security.

The first seven proposed AI factories in the EU have been presented

The European Commission's main goals include the creation of the first artificial intelligence factories in early 2025. These factories are intended to create a thriving European ecosystem for training advanced AI models and creating AI solutions around existing and new supercomputers in the EU. They will also bring together the key ingredients for the success of AI, namely computing power, data and talent.

While driving AI innovation throughout the EU, these factories foster collaboration and advancements in this field, by offering avant-garde resources to European AI startups, to industry and to researchers in various key sectors such as health, energy, manufacturing or meteorology.

The Commission has reviewed seven proposals submitted by 15 EU member states, including Spain, and two associated participating states (Norway and Turkey). These proposals submitted under the EuroHPC Joint Undertaking (JU), managing the call for expressions of interest announced in September 2024, will be analyzed by an independent group of experts. The EuroHPC Joint Undertaking is expected to announce the first AI factories in December 2024 and bring them into operation shortly afterwards.

Meta launches a new advertising model

Meta has launched a new model in its apps, which features an option for users to (i) subscribe to use the apps with no targeted ads; or (ii) continue using the apps for free, and therefore the user's data can be used to provide targeted ads; or (iii) use the apps for free and receive targeted ads although a smaller number and based on less detailed information.

This third option is the new option included in the model, and, according to information published by the company itself, it consists in showing adds based only on contextual information from each user session. In other words, personalizing adds based on the content seen by each data subject in a session using the app.

The new model has been commented on widely in the sector and is not completely without controversy. Its functioning and implementation will have to be analyzed in detail to assess all its implications from the standpoint of the applicable legislation and the EDPB guidelines in relation to this type of personal data processing.

New cybersecurity requirements have been approved for products with digital elements

Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) was published on November 20 in the Official Journal.

This new regulation sets out the cybersecurity requirements for products with digital elements. It came into force on December 10, 2024 and became applicable on December 11, 2027, with notification obligations starting on September 11, 2026.

The aim is to ensure that connected products like domestic cameras, fridges, televisions and toys are secure before they are placed on the market. This regulation seeks to cover shortfalls in the rules in force on cybersecurity, clarify the links with that legislation and achieve greater coherence, by ensuring that products with digital components are secure throughout the supply chain and over their life cycles.

The regulation will apply to all products connected directly or indirectly to another device or to a network, with some exceptions

for products that already have cybersecurity requirements in other pieces of EU legislation, such as medical devices, aeronautical products and vehicle components and systems.

The new legislation will also allow consumers to take cybersecurity into account when choosing and using products with digital elements, because obligations are laid down for manufacturers to inform on these characteristics, by facilitating the election of hardware or software products with adequate cybersecurity characteristics.

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

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

Antonio Durán
Associate · Málaga
antonio.david.duran@garrigues.com

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

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

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

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

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

For more information:

Data Economy, Privacy and Cybersecurity

GARRIGUES

Hermosilla, 3
28001 Madrid
T +34 91 514 52 00
info@garrigues.com

Follow us on: