GARRIGUES

Data Economy, Privacy and Cybersecurity Newsletter

October 2024

Contents

1. The regulatory and supervisory labyrinth in the digital agenda for Europe: rationalization proposals

The publication of the Artificial Intelligence Act has brought a complex regulatory framework for overseeing the use of AI, with surveillance and supervisory authorities that overlap and co-exist with others in the digital economy. In its quest for efficient governance that is coherent with other regulations such as the GDPR, the European Data Protection Board (EDPB) recommends that the data protection authorities perform supervisory functions in order to avoid a dispersal of public authorities.

Alejandro Padín Vidal

The recent publication of the Artificial Intelligence Act is one of the main regulatory achievements in the field of the digital economy, also known as the information economy or data economy. From a structural standpoint, it is an extremely complex piece of legislation that seeks to regulate the use of AI systems; a novel and changing area. The contents regulated in the Act include a governance and supervisory structure that establishes the creation of various competent authorities both at a national level in each member state, as well as at EU level.

The approach makes perfect sense, because an act that implements the obligations of the affected entities to such an extent must go hand-in-hand with an adequate verification of its application. However, if we look at the matter from a wider perspective, it is evident that the authorities envisaged in the AI Act, join another array of supervisory, governance, surveillance and registration authorities that have been created in several European regulations that have been adopted in connection with the digital agenda for Europe over the last few years. Supervisory and/or surveillance and/or registration authorities have been created, at times with powers to impose penalties, in the GDPR, the Data Regulation, the Data Governance Regulation, the NIS 2 Directive and the DORA Regulation, to name but a few.

This reality, which the world of business may view as a disproportionate increase in administrative formalities and red tape, could be mitigated, if efficiency and specialty criteria are applied, to ensure that the various supervisory functions are assumed by the same authority with similar or related functions.

In this regard, the EDPB has published a statement in which, with regard to the AI Act, it affirms that it is advisable for the data protection supervisory authorities created by the GDPR to assume the duties of the market surveillance authority. This is based on the recognition that the Act and European privacy rules such as the GDPR or the e-Privacy Directive, should be considered and interpreted coherently as supplementary instruments that provide mutual support.

This recommendation by the EDPB is related to the statement that data protection (both personal and non-personal) in the lifecycle of an AI system, especially high-risk systems, is clearly central to the different technologies covered by the umbrella of the definition of AI in the Act. In addition, as the EDPB held in its Joint Opinion with the European Data Protection Supervisor (EDPS), it is also related to the experience already gained by the supervisory authorities in connection with AI, the benefits of implementing a single point of contact for market operators and their degree of independence, which furthermore avoids possible discrepancies between the decisions of both supervisory authorities.

Since some Member States (such as Spain) have initiated legislative processes for the creation of these supervisory authorities contemplated in the AI Act alongside the data protection supervisory authorities, the EDPB remarked on the importance that the entities should collaborate in future processes based on article 4(3) of the Treaty on European Union.

In short, the EDPB recommends that data protection supervisory authorities should be designated, in countries where they still do not exist, such as the market surveillance authorities for the high-risk AI systems mentioned in the AI Act.

In our opinion the digital economy should move towards an aggregation of functions, in order to avoid an excessive dispersal of supervisory, inspection and penalty bodies, which would ultimately place a barrier on the appearance and progress of market operators.

2. Data protection authorities' decisions

The Spanish data protection agency (AEPD) fines a bank €70,000 for providing tax information to the ex husband of the owner of financial products

The complainant stated that, without her consent, the bank had provided her ex husband with tax information for 2021 on all the bank's products she owned. The bank submitted that both the complainant and her ex husband appear on its systems as joint owners of the product, which is why access was gained to all the tax information of the two owners and the Single Tax Certificate was delivered to the complainant's ex husband, thereby incurring what it classes as an "inadvertent human error".

In its decision PS-00143-2023 of July 11, 2024 the Spanish data protection agency (AEPD) held that a personal data breach had taken place (namely, a breach of confidentiality), because the data had been unlawfully disclosed to third parties. It noted moreover that the fact of the event occurring through an individual and isolated action of an employee acting against the internal rules does not relieve the data controller of its liability for compliance with the data protection legislation.

The decision stresses that in addition to the need for a set of rules and an ongoing employee training and awareness program, other technical and organizational measures need to be adopted which contribute to reducing the specific risks arising from the particular characteristics of the processing. It notes in fact that if additional measures have been adopted as a result of this procedure aimed at avoiding incidents such as the one that occurred, it is because the security measures in place were insufficient or not robust enough.

Another issue that the decision addresses is infringement of the *non bis in idem* principle, which, it concludes, does not exist in this case, because article 5.1 f) (principle of integrity and confidentiality) and 32 (security of processing) of the GDPR seek different aims, although they may be connected.

The AEPD concluded therefore that the bank had not fulfilled its owed duty of care for which the AEPD gave particular weight to the professionalism required of the infringing party and the connection of its activity with the processing of personal data. It imposed a €50,000 fine for infringement of article 5.1 f) of the GDPR and another €20,000 fine for infringement of article 32 of the GDPR.

The AEPD recalls that personal data obtained from the Industrial Property Official Gazette (BOPI) cannot be used by third parties to send advertising material

Decision PS-00206-2024 of July 12, 2024 relates to a case in which the complainant received advertising mail from a company with which it had not had any commercial relationship or any prior contact. The data used in the communication came from the Industrial Property Official Gazette (BOPI) and the purpose of the communication was to attract the complainant as a client.

To respond to the complaint, the AEPD used a report from the legal services office drawn up at the request of the Industrial Property Agents Association and reached the following conclusions:

- The personal data were published in the gazette under a legal mandate. In other words, the publication of the complainant's personal data in the gazette took place because the law so required, not because the complainant had voluntary decided to make those data public.
- The use made of the personal data departed from the statutory purpose for their publication in the BOPI, which consisted of allowing other interested parties in the grant, concession or denial, etc. of the industrial property right to object, if they so decide. However, the respondent processed the data for the purpose of sending an informative postcard offering its services.
- The processing was not foreseeable for the complainant.
- The informative postcard sent by the respondent must be seen as being addressed to the complainant as a private party, not as a company representative.
- In the examined case, the respondent cannot rely on the exception contained in article 9.2 e) of the GDPR, because no special categories of data were involved.

Therefore, it was held that the processing of personal data was carried out without a lawful basis from among those set out in article 6.1 of the GDPR and the penalty proceeding was initiated, which ended with voluntary payment by the respondent company.

If rights are to be exercised all the affected personal data must be retained

In its decision PS 131/2023 the AEPD fined a department store group €140,000 for infringement of GDPR articles 15 on right of access and 18 on restriction of processing. The fined company did not comply correctly with the complainant's request to retain and give it access to security camera footage of the accident suffered by a minor on that company's premises, in case it had to be submitted as documentation in a potential claim for damages.

In its decision, the AEPD stated that all personal data that may be useful for exercising rights must be retained, that it is not up to the controller to determine whether they are relevant, and the necessary clarification must be sought before erasure.

The AEPD also noted that, on this occasion, it was fully justifiable for the respondent to go over the retention period for footage recorded by the company itself (15 days), because complying with the rights exercised by the complainant must prevail.

Lastly, the AEPD ruled that, in this case, the right of restriction does not arise from the right of access, and therefore a separate fine must be imposed for each infringement.

It is prohibited for workers to clock in using facial recognition systems at public institutions

A complainant brought a complaint with the AEPD against a local authority, seeking to have the AEPD examine the lawfulness of

imposing a facial recognition system as a time tracking method for that local authority's employees, and review whether a prior impact assessment of biometric data processing had been carried out.

In a decision dated June 21, 2024**,** the AEPD held it had not been substantiated sufficiently whether any of the exceptions contained in article 9.2 of the GDPR applied, allowing biometric data to be processed as a means of overseeing the legal obligation to track and monitor the time worked by local authority employees.

Therefore, in this case the AEPD ordered suspension of all the data processing related to the biometric time clocking systems. It also gave the local authority seven months in which to perform a data processing impact assessment with the associated prior risk assessment, in addition to an assessment of the triple suitability, necessity and proportionality test on those time clocking systems, to determine whether any of the exemptions under article 9.2.of the GDPR apply, as well as to put in place adequate protection measures and to fulfill all the other obligations required under the data protection legislation.

The AEPD fines a company for human error in the sending of employees' pay statements

After requesting his pay slip from his employer's HR department, a worker received an email with a PDF document containing his pay statement along with those of 446 other staff members. Besides the amounts it also contained particulars such as the names, surnames, national identity card numbers, social security numbers and bank account numbers of the 447 workers.

The company admitted to the facts described in the complaint and pleaded that the personal data breach had been caused by human error in the sending of the file, in addition to which the HR employee that sent the file had not reported it to his superiors or informed the company. For that reason, according to the respondent, the breach did not come to light and it was unable to react proactively to it. After learning of the events, the company implemented a threat intelligence tool and its internal procedures for sending pay statements were reviewed.

Despite the adopted measures, in its decision the AEPD imposed a €300,000 fine for a purported infringement of article 5.1.f) of the GDPR (on confidentiality), and a €150,000 fine for a purported infringement of article 32 of the GDPR, because evidence had been provided of the absence of sufficient security measures, as defined in article 83.4.a) of that regulation.

Fine in the millions given out by the Dutch authority to a private hire firm for an international transfer of drivers' data to the U.S.

More than 170 French drivers working for a Dutch private hire firm filed a complaint with the French human rights association *Ligue des Droits de l'Homme* (LDH). The French supervisory authority sent the complaints to its Dutch counterpart.

An investigation uncovered that the private hire firm collected, among other things, sensitive information belonging to European drivers and stored it on servers in the U.S. That information contained particulars on bank accounts and taxi licenses, along with location data, photos, payment details, identity documents, and in some cases, drivers' criminal offense and medical data.

Over more than two years, between the judgment invalidating the *Privacy Shield* agreement and the approval of its successor, the private hire firm transferred all those data to its offices in the U.S., without using transfer tools. For that reason, on July 22, 2024 the Dutch authority handed out a €290 million fine to the company**.**

An IP address is not sufficient proof due to the high vulnerability to cyberattacks of domestic routers

The complainant reported that someone had published an advert with her photo and phone number offering sexual services, and various people had contacted her as a result. The AEPD investigated the websites involved, but they no longer showed the adverts. It therefore requested information from the data controllers and obtained an IP address linked to those adverts. It later sent a request to the owner of the IP address for justification of the publication, although no reply was received.

During the procedure, the respondent pleaded that several family members used the same computer and the same connection, as well as that the security of domestic routers was not inviolable, supporting its defense with a supreme court judgment dated December 3, 2021, appeal 2429/2011, which acquitted the accused due to the high vulnerability to cyberattacks of his internet connection.

In its decision PS 297/2023, the AEPD dismissed the case on the grounds that (i) the respondent lived with other individuals who could have used his connection, (ii) there were discrepancies over the publication dates of the advert, and (iii) it is unlikely that the respondent, who was 75 and lived at a care home at the time of the events, published the information by himself. Therefore, the respondent's liability could not be proved and the case was dismissed.

A channel set up for answering workers' queries is an adequate channel for receiving right of access requests

In its decision PS 168/2023, the AEPD fined an online home delivery platform €15,000 for not having replied adequately to a right of access request made by a worker.

The respondent pleaded that it could not be held liable, because the worker exercised his right of access via a support email address, rather than via the official email address for privacy related matters, which was the address specified in the Privacy Policy. It also pleaded that adequate internal mechanisms had been implemented to ensure that this request was resent to the suitable channel, and by doing so it was fulfilling its duty to make a reasonable effort, due to this being a best efforts obligation.

The Agency held that the channel used by the complainant was a valid means, proved by the fact that the respondent had already put in place a procedure for those requests to be resent to this channel related to data protection matters. It clarified, lastly, that because it is not disproportionate to ask a customer services department to handle this type of request, it cannot be held that the respondent made reasonable efforts.

Making entry to an establishment conditional on consent being given for the processing of data is an infringement of article 4.11 and article 7 of the GDPR

The complainant reported a theme park for making the signing of a form authorizing the company to capture images for advertising purposes a condition for entering its premises, and the complainant was obliged to give her consent so that her son who is a minor could be allowed entry. At the end of that form only one box was provided to tick "OK" and no option was given for withholding consent.

In decision PS 104/2023, the AEPD referred to article 4.11 of the GDPR, which defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she signifies agreement to the processing of personal data relating to him or her. Article 7 of the GDPR adds that the controller must be able to demonstrate that consent was given, and that consent may be easily withdrawn, and the purpose for which the consent was requested must be clearly distinguishable from the other matters on the forms.

In the case brought to the agency, it was held that the park infringed article 7 by making entry

to its premises conditional on signing consent which was neither freely given nor specific. As a result, the Agency handed a €2,000 fine for infringement of article 7 of the GDPR.

Whether an entity is data controller or data processor depends on the specific circumstances, and the parties cannot arbitrarily decide its role

The AEPD has published a penalty proceeding decision giving out two fines of €2,500,000 each, for separate infringements of article 5.1.a) (principle of fairness and transparency) and article 5.2. (accountability) of the GDPR. This is a particularly important decision because it contains a systematic description of an array of concepts and obligations concerning almost all the parties with obligations under the data protection legislation in their daily operations.

The decision examines the processing of personal data by an energy retail company that uses a third party for the telemarketing of its products and services. The telemarketing firm made marketing calls to attract customers on behalf of the retail company. According to the decision, fraudulent practices were used in these calls to increase the number of customers they attracted, by using misleading information, causing confusion among the contacted individuals and breaching the transparency obligations imposed by the GDPR.

The respondent argued that the calls were made by the telemarketing firm and it was responsible for them, but, in its decision, the AEDP, citing the conclusions in guidelines 07/2020 on the concepts of "data controller" and "data processor", states that the controller role lay with the respondent, because a sales pitch had been imposed by it, and there were clear and documented instructions on how to sell its services, so the telemarketing firm acted as data processor. The AEPD concluded that whether an entity acts as data controller or processor depends on the specific circumstances of their actions and the parties cannot decide its role arbitrarily as suits them.

The AEPD stressed the need for exhaustive, constant and thorough monitoring by data controllers, and that they must document and keep evidence of their actions so that they can prove this has been done.

Lastly, the AEPD held that breaches of the fairness and transparency and accountability principles set out in article 5 of the GDPR are sanctionable in themselves, without needing to fall within more specific definitions of infringements, and that this does not breach the principle of legal definition.

The AEPD changes its opinion and holds that delivering a parcel to a third party should not be subject to a fine

The AEPD has delivered a number of decisions (EXP202314031, EXP202313840, EXP202313995 and EXP202314242) from which it may be inferred that it has changed its criterion over courier companies' practice of delivering parcels to third parties other than the originally intended recipient.

Recently, in a similar case the AEPD handed a €70,000 fine to a courier company, whereas in this string of new decisions, the AEPD has held that delivering a parcel to a neighbor, local business to the intended recipient or the janitor of a multi-residential building does not warrant a fine.

The AEPD noted that, although it is true that the delivery of parcels to these parties means disclosing personal information belonging to the intended recipient without their permission, these particulars will usually only consist of their name, surname and address, and this information is already known by the person receiving the parcel on behalf of the intended recipient. For that reason, the AEPD held that this practice is of little consequence and dismissed the cases without a fine.

3. Judgments

A legal guardian, with responsibility for protecting and managing the interests of a person in their care, is data controller, even if they form part of that person's inner circle

The Court of Justice of the European Union (CJEU), in a judgment dated July 11, 2024 (C-461/22), construed that the activity of a professional guardian, even if the guardian is a member of the ward's personal circle, implies that they are controller of the personal data of that person in their possession, and the resulting obligation to comply with all the applicable provisions of the GDPR, including allowing the data subject to exercise their right of access under article 15 of the GDPR.

That judgment took place after a German citizen under guardianship exercised his right of access under article 15 of the GDPR to data collected by his former guardian, a lawyer appointed in a professional capacity. The referring court submitted a question for a preliminary ruling as to whether the guardian could be classified as data controller from the standpoint of the data protection legislation.

Associations can claim breach of the right to information on behalf of the interested party, where it is regarded as an infringement "as a result of the processing"

A major technology company and the German Federation of Consumer Organizations and Associations became involved in a lawsuit over the former's purported infringement of the German data protection legislation, which constituted, at the same time, an unfair commercial practice, an infringement of a law relating to consumer protection and a breach of the prohibition of the use of invalid general terms and conditions. In this context, the referring court asked whether, on the basis of article 80.2 of the GDPR, an association would be entitled to base a complaint on an infringement of the prior right of information, considering that it was not strictly an infringement of a right "as a result of the processing".

In this case, in a judgment dated July 11, 2024 in case C-757/22**,** the Court of Justice of the European Union (CJEU) ruled that the information obligation forms part of the rights that article 80 seeks to protect and failure to comply with that obligation infringes the principle of fair and transparent processing, in addition to precluding the expression of free consent. It must therefore be regarded as an infringement of the data subject's rights "as a result of the processing". Moreover, the data controller must provide the data subject, in a concise, transparent, intelligible and easily accessible

form, in clear and plain language, with information relating to the purposes of that data processing and to the recipients of such data, at the latest when they are collected.

A €250,000 fine by the AEPD has been overturned, after being given out for enabling the microphone and geolocation in apps on users' mobile pones

In a decision dated June 10, 2019**,** the AEPD fined a professional organization €250,000 for infringing the transparent processing principle under article 5.1.a) of the GDPR, in relation to the use of certain functions of its official app. The reported fact was related to microphones and geolocation on mobile devices to detect fraud over the audiovisual contents of football matches.

The Supreme Court, in a decision dated July 15, 2024, confirmed that the information provided on downloading the app meets the requirements contained in the GDPR. It clarified, however, that the transparency principle applies where that app collects personal data, both at the point when it is installed and over prolonged periods of time without any prior notification.

The Supreme Court interpreted the limits of the duty of transparency and connected them with the scope of the AEPD's power to impose sanctions, stating that:

a. The duty of transparency must be tailored to the specific circumstances of the processing. In this case, the transparency obligation applies both on installing and on running a mobile app because prolonged use may mean that users forget the information and additional mechanisms are needed.

b. The AEPD may require the existence of a specific notification on mobile phones each time the microphone is enabled, due to being regarded as a proportionate measure.

c. However, the requirement for this specific notification is not expressly provided for in the GDPR nor does it transpire from Organic Law 3/2018 of December 5, 2018. AEPD's power to impose sanctions is governed by the foreseeability principle, and therefore the AEPD cannot increase the scope of the transparency requirement to limits that are unforeseeable.

d. It was not reasonable to take for granted that the transparency principle required a privacy notification each time the app enabled the mobile phone's microphone. The AEPD cannot directly impose a sanction for an infringement of guarantees determined after the event and which were not foreseeable when the conduct took place.

In conclusion, the Supreme Court found that the principle of transparency was met in the processing of personal data obtained via the app, because the requirement to include a specific information notification was not foreseeable. It therefore overturned the sanction imposed by the AEPD.

Colombia's Constitutional Court clarifies that artificial intelligence cannot replace the judge in decision making

In its decision on action filed for protection of fundamental rights, the Colombian Constitutional Court made important determinations on the use of artificial intelligence by judges when deciding on court proceedings.

In judgment T-323 delivered in 2024, the court concluded that artificial intelligence cannot replace the judge in the making of court decisions, however complex the case. Therefore, the use of these systems is feasible for administrative or documentation procedures, although not for tasks involving content creation or interpretation of facts or items of proof, and much less so for settling cases.

The supervisory authority is not under obligation to adopt corrective measures in all cases of infringements or to impose a fine

The Court of Justice of the European Union (CJEU) has ruled in case C-768/21, originated in Germany after a savings bank employee unlawfully accessed a customer's personal data, that the supervisory authority is not required to adopt corrective measures in all cases. The savings bank did not inform that customer that there was a security incident that affected the personal data of an individual, since its data protection officer had taken the view that there was no high risk to the customer's rights because the employee confirmed in writing that she had neither copied, retained, nor shared the personal data, and that she would not do so in the future. Moreover, the savings bank took disciplinary measures against her and notified the data protection commission for the federal state.

Following notification to the data protection supervisory authority, it considered that it was not appropriate to impose corrective measures, in view of the measures that the bank had adopted. The customer, not satisfied with the situation, lodged an action with a German court, asking it to order the supervisory authority to take action against the savings bank and impose a fine.

In its judgment, the CJEU held that the data protection authorities are not under obligation to adopt corrective measures in every case of a GDPR infringement. A fine does not need to be imposed if the data controller has taken appropriate measures at its own initiative to bring the infringement to an end and ensure that it does not recur.

The CJEU concluded that the supervisory authorities have an amount of discretion in deciding how they must remedy the shortcomings found, as long as a consistent and high level of protection of personal data is ensured. Whether the supervisory authority observed those limits is a matter for the German court to determine.

4. News update

The EU Artificial Intelligence Regulation has been published in the Official Journal

On July 12 the Official Journal published the Artificial Intelligence Regulation (AIR); an act that will not be generally applicable until August 2, 2026, in other words, 24 months after its entry into force on August 2, 2024.

A few provisions in the regulation are applicable in other periods. Prohibitions against certain AI practices, for example, will come into force earlier on February 2, 2025.

The provisions on notified bodies, general-purpose AI models that pose systemic risks, the AI governance system in Europe and a large part of the panoply of penalties, will become applicable on August 2, 2025. This means that the organizational base will be ready for when the more substantial set of obligations become enforceable.

Lastly, the rules on certain high-risk AI systems (safety components of products, or which are themselves products and require a conformity assessment in order to be placed on the market or put into service i.e. machinery, toys, lifts or medical devices) will become applicable on August 2, 2027.

The Spanish data protection agency has presented a report on the influence of addictive patterns in online services, especially on minors

A report by the Spanish data protection agency highlights how the providers of a high number of platforms and applications implement misleading and addictive design patterns to lengthen the time users spend on their services, or to increase their level of commitment and the amount of personal data they collect about them.

This adverse impact of addictive strategies is considerably greater when they are used to process personal data of vulnerable individuals, such as children and teenagers.

The AEPD will recommend that the European Data Protection Board include addictive patterns in the guidelines they are preparing on the interplay between the GDPR and the DSA, due to the high impact these practices have on data protection rights in digital environments.

The EDPB recommends that data protection authorities are designated as supervisory authorities of the Artificial Intelligence Regulation

This statement by the European Data Protection Board (EDPB) has been prompted primarily by the experience already gained by the data protection authorities in AI matters, the benefits of making available a single point of contact for market operators, and their degree of independence, in addition to preventing any inconsistencies between the decisions of both oversight authorities.

Because a few member states have started legislative processes for the creation of those supervisory authorities under the Artificial Intelligence Regulation to exist alongside the data protection supervisory authorities, the EDPB highlights the importance of the authorities collaborating and cooperating with each other in future processes on the basis of article 4(3) of the Treaty on European Union.

The EDPB allows EU institutions to use generative AI systems if they are compliant with the data protection legislation

The European Data Protection Board (EDPB) has published its first orientations for ensuring data protection compliance for EU institutions, when using Generative AI systems. They provide practical advice and instructions on the processing of personal data in these cases.

Broadly speaking, they allow EU institutions to use Generative AI systems provided they are compliant with the applicable legislation, particularly the data protection legislation.

The orientations also address important issues such as the role played by data protection officers in the implementation of Gen AI systems, how to apply the data minimization principle, or how to inform interested parties about the processing of their personal data.

The AEPD issues guidelines on safe online purchasing in conjunction with the Spanish National Cybersecurity Institute (INCIBE), the Spanish Agency for Consumer Affairs, Food Safety and Nutrition (AECOSAN) and the Spanish National Police Force (*Policía Nacional*)

In view of the widespread use of e-commerce, the AEPD has released a practical guide on safe online purchasing setting out users' rights in online purchasing processes and providing advice and recommendations in relation to privacy, security, consumer affairs and the persecution of fraudulent practices.

The guide is divided into sections. The AEPD first provides recommended good practices before starting online purchases to help users identify fraud and fake websites, as well as avoid falling prey to phishing.

Next the guide highlights the main components of the security provided by the usual payment methods in e-commerce (bank transfers, card payments, etc.).

In the third section, the AEPD covers the array of rights and guarantees available to users in online purchasing processes (right of withdrawal, personal data rights, among others).

And lastly, in the section entitled "How to complain", the guide provides recommendations on the channels where users can lodge complaints in the event of a breach of any type of legislation.

The OECD has published a report on regulatory approaches to artificial intelligence in finance

The policy paper looks, among other things, at different regulatory approaches to the use of AI in finance in 49 OECD jurisdictions and non-OECD jurisdictions based on a survey on regulatory approaches to AI in finance.

The report notes that the majority of jurisdictions have adequate regulations on AI in finance, while acknowledging that there may be some gaps such as an absence of specific regulations which few regulators have issued.

The Council of Europe has signed a Framework Convention on artificial intelligence and human rights, democracy, and the rule of law

It is the first legally binding international treaty and is aimed at "ensuring that activities within the lifecycle of artificial intelligence systems respect equality, including gender equality, and the prohibition of discrimination, as provided under applicable international and domestic law."

This framework convention applies to both public authorities and private entities, and provides for an oversight mechanism to ensure compliance, which includes international cooperation between the party states. Each state has flexibility over applying the convention in their legal system, although they must implement measures tailored to the risks of AI systems. The convention does not cover technology however and is essentially neutral on technology matters.

The European Commission has published a document to help companies learn about their obligations in relation to the Data Act

The EU's new Data Act (Regulation (EU) No 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data) will become fully applicable on September 12, 2024, and together with the Data Governance Act (Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance) is aimed at increasing trust in data sharing mechanisms in the EU.

The European Commission has published a set of FAQs on this subject to help companies understand their obligations in further detail. The main topics covered are a) how the act interacts with other European laws, b) questions about the Internet-of-Things (IOT), c) considerations about users, data holders and other third parties involved, and d) establishing fair, reasonable and non-discriminatory conditions, compensation and dispute resolutions mechanisms.

The Belgian data protection authority has published a guide on the use of artificial intelligence models and the General Data Protection Regulation

The topics covered in this document include a) a definition of AI systems, b) the requirements for these systems to be compliant with the GDPR, c) the safeguarding of data subject rights through the use of AI systems, and d) the requirements for complying with the GDPR principles, keeping data up-to-date and ensuring secure processing.

The guidelines summarize the key points to be taken into account when addressing this technology from the perspective of GDPR compliance.

The AEPD releases guidelines on obligations and responsibilities in the use of mobile digital devices at educational centers

The use of mobile phones, tablets and smart devices in classrooms has grown exponentially over recent years which has created risks for the protection of pupils and students. With this in mind, the AEPD has published a paper with guidelines on responsible use of these devices and compliance with the data protection legislation.

It notably advises against the use of these devices in schools, where the sought educational goal may be achieved using a more suitable resource. In this agency's view, the use of smart devices at schools must pass the suitability, necessity and proportionality test.

The AEPD recalls moreover that any data processing that departs from the purpose for which the data was collected must be regarded as unlawful, and may result in liability, not just in an administrative sense for infringements of the data protection legislation, but also in liability for damages and losses, and in some cases the institutions and education authorities could be held jointly and severally liable.

Chile: Legislative step forward and impacts of the new Personal Data Law

The new Data Protection Law approved by the Chilean parliament (Congreso Nacional de Chile) on August 26 regulates data processing and strengthens data subjects' rights, in alignment with GDPR. One of the main new provisions is the creation of the Data Protection Agency, tasked with overseeing compliance with the legislation and running the National Sanctions and Compliance Register which will record the sanctions imposed on companies.

The new law increases data subjects' rights which will include data portability and erasure. It also requires companies to carry out data protection impact assessments where a type of processing (due to its nature, scope, context, the used technology or aims) can pose a high risk to data subjects' rights.

Equally notable are the duties it places on data controllers, such as the duty of secrecy, information and transparency, together with the obligation to put in place adequate data processing policies and security measures. Along the same lines, there are tougher sanctions for non-compliance, with fines of up to 20,000 UTM (US$1,418,000), which can be tripled for a recurring infringement.

The new law is set to come into force 24 months after its publication in the Official Gazette.

Colombia: Personal data administrators using AI systems must assess the suitability and necessity of the data processing

To ensure adequate compliance with Law 1581 of 2012, the Industry and Trade Authority released guidelines for personal data administrators using artificial intelligence systems.

Among other obligations, anyone using these systems will have to assess the suitability, necessity, reasonability and proportionality of the data processing. On top of this, privacy impact studies will have to be carried out and risk management systems will have to be implemented before the design and development of any AI system. External Circular No 002 of 2024 is available here.

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

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

Adolfo Gómez
Senior associate · Colombia
adolfo.gomez@garrigues.com

For more information

Data Economy, Privacy and Cybersecurity - Lawyers | Garrigue

GARRIGUES

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

Follow us on: