MOLINS

Defensa Penal **Compliance**

Compliance Newsletter

July 2024

Index

Introduction

Compliance is essential to ensure the integrity and sustainability of organisations in today's complex and changing regulatory environment. Staying informed is more than an obligation: it is a **strategic imperative** to ensure the proper and continued progress of businesses.

Throughout the first half of 2024, we have seen important developments in Compliance. These include developments in sustainability and corporate responsibility, as well as increasing regulation around data protection and privacy. At the same time, significant legislative changes have been introduced, relevant decisions have been issued by the Supreme Court and other courts, and numerous reports and guides of interest have been published by various authorities in the field.

The Departament of Compliance in **Molins Defensa Penal** has prepared this newsletter as a compilation of the most significant milestones in matters of Compliance in the last six months. Its content is as follows:

- **Key legislative developments** with an impact on the design of Compliance Systems will be analysed.
- This will be followed by a number of recent **Supreme Court and Constitutional Court decisions of interest in the area of Compliance.**
- Other important agreements and sanctioning decisions in the area of Compliance will also be examined.
- This will be followed by a brief presentation of various **guidelines, institutional resolutions and reports** of interest in the area of Compliance.
- This newsletter will conclude with the Department of Compliance **catalogue of publications** for the first half of 2024.

New legislation

- Corporate Sustainability Due Diligence Directive (EU) 2022/2464 (CSDDD)
- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER)
- The new 'Foreign Extortion Prevention Act' (FEPA)
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
- Draft Royal Decree approving the Statute of the Independent Whistleblower Protection Authority
- New EU AML and CFT package of rules, 30 of May 2024
  - Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing
  - Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (AMLA)
  - Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849Text with EEA relevance.
  - Directive (EU) 2024/1654 of the European Parliament and of the Council of 31 May 2024 amending Directive (EU) 2019/1153 as regards access by competent authorities to centralised bank account registries through the interconnection system and technical measures to facilitate the use of transaction records:
- Regulation of the European Parliament and of the Council on Artificial Intelligence - AIA).

New legislation

MOLINS Compliance

Corporate Sustainability Due Diligence Directive (EU) 2022/2464 (CSDDD)

The **CSDDD** establishes **reporting obligations and sustainability due diligence measures** for organisations, addressing three specific dimensions: **environmental, social and governance**, known as **ESG**.

The Directive obliges organizations to address adverse impacts on human rights and the environment arising from **their own operations, those of their subsidiaries and those of their business partners**. These obligations are intended to comply with the **European Green Deal** and are based on the **European Sustainability Reporting Standards.**

Organizations must therefore implement **diligent human rights and environmental risk management systems** and report on these in their sustainability reports.

The **monitoring of compliance with the provisions of the CSDDD** will be carried out by the relevant specialized body of the public administration with the following powers:

- Power of **investigation**.
- Adoption of **precautionary measures.**
- Imposition of **sanctions.**

What self-regulatory standards can organisations adopt to facilitate compliance with these obligations? The following, among others:

- **Environmental dimension**: UNE-EN ISO 14064-1 on greenhouse gases (inventory) and ISO 59020 on measuring and assessing circularity performance, among others.
- **Social dimension:** regulations aimed at ensuring a stable working environment, such as the UNE 19604 for management system for socio-labour compliance.
- **Good governance:** in the criminal area, the UNE 19601 standard for management system for criminal compliance; in the tax area, the UNE 19602 standard for tax compliance management systems; in the area of corruption prevention, the ISO 37001 standard for anti-bribery management systems, among others.

This Directive will enter into force on **26 July 2024.**

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER)

The CER Directive aims to **establish specific harmonised measures to ensure the unobstructed provision of services essential for the maintenance of vital societal functions or economic activities**. This is done by **improving the cyber resilience of critical entities** and enhancing **cross-border cooperation**.

Cyber resilience is the ability of an entity to protect, resist, mitigate, absorb, adapt and recover in the event of an incident (it goes beyond cyber security).

The CER Directive establishes, among others, obligations in the following areas:

- Duty of **risk assessment.**
- **Resilience-cybersecurity measures, response, recovery, etc.**
- **Background checks**.
- **Incident reporting.**

The CER Directive applies to **critical entities, which must be identified by the Member States on the basis of the following criteria**:

- Entities providing **one or more essential services;**
- Entities that operate on the **territory of that Member State and their critical infrastructure is located there,** and
- Entities which, **in the event of an incident**, would cause significant disruptive **effects on the provision of one or more essential services, or on the provision of other essential services dependent on that service.**

The deadline for transposition of this Directive is **17 October 2024.**

New legislation

MOLINS Compliance

The new 'Foreign Extortion Prevention Act' (FEPA)

The **FEPA** complements the Foreign Corrupt Practices Act and establishes, for the first time, **criminal liability for foreign officials** who solicit or accept bribes from persons or entities to which the Foreign Corrupt Practices Act applies (the demand side is sanctioned).

It is noteworthy that the effects of this regulation are **not limited to the territory of the United States** but extend to the **solicitation and acceptance of bribes by foreign officials when they have a nexus to the United States.**

Foreign officials who violate FEPA could face a penalty of up to $250,000, three times the value of the bribe, imprisonment for up to 15 years, or both.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

The **NIS 2 Directive** lays down measures that aim to **achieve a high common level of cybersecurity** across the Union with the objective of **improving the functioning of the internal market.**

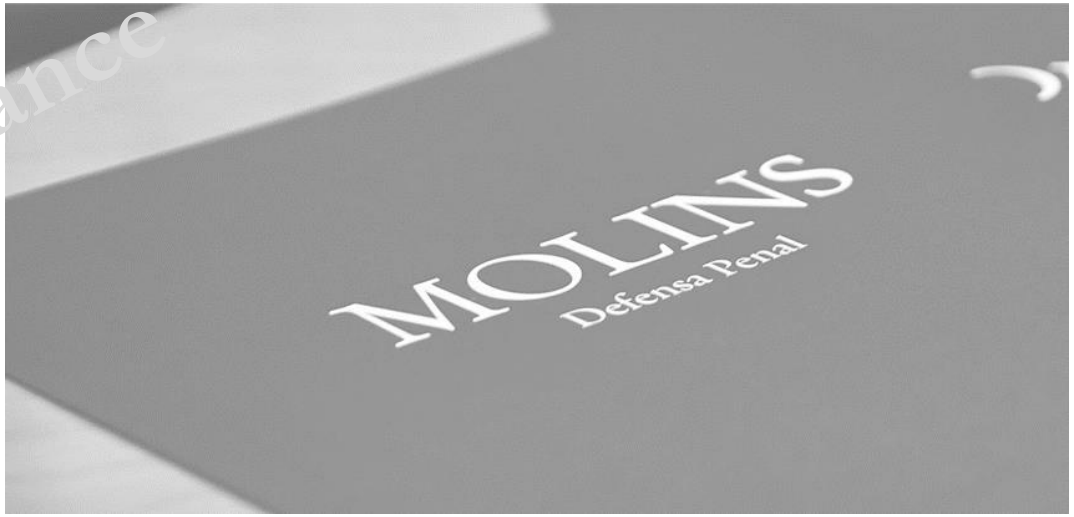
To this end, the Directive provides for:

- The state obligation to adopt a **national cybersecurity strategy**.
- **Cybersecurity risk management measures and notification obligations for obliged entities.**
  - These are regulated in **Article 21** and include, among others, **incident** management; **cyber hygiene policies** and **cybersecurity training**; the use of **multi-factor authentication or continuous authentication systems**; and **security in the supply chain**, including **security** aspects of the relationship between entities and their suppliers.

Broadly speaking, the NIS 2 Directive applies to **a total of 18 sectors** (Annex I and II), divided into:

- **High criticality sectors:** energy; transport; banking; financial market infrastructures; health; drinking water; waste water; digital infrastructure; ICT service management (B2B); public administration (excluding the judiciary, parliaments and central banks); and space.
- **Other critical sectors**: postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; manufacturing; digital providers; and research.

The deadline for transposition of this Directive is **17 October 2024.**



New legislation

MOLINS
Compliance

Draft Royal Decree approving the Statute of the Independent Whistleblower Protection Authority

The **Independent Whistleblower Protection Authority (A.I.I., for its acronym in Spanish)** is a state body with **autonomy and functional independence** whose objective is to comply with the **mandate of Law 2/2023.**

The **functions** of the A.I.I. are as follows:

- **Processing of information and communications** carried out through the external channel of the A.A.I. itself.
- Adoption of **protection and support measures** for whislteblowers.
- **Initiation, instruction and resolution of sanctioning procedures.**
- Drawing up **circulars (of a binding nature) and recommendations**.
- Establishing **collaboration relations with other similar authorities** (e.g.: Anti-Fraud Office of Catalonia).
- To draw up an **annual report and aggregate statistical information**.
- Contribute to the **creation and strengthening of an information culture**.

One of its **most relevant functions** is to sanction **breaches of the whistleblower protection provisions of Law 2/2023.** Despite this, the A.A.I. cannot exercise the functions of judges or prosecutors (it cannot investigate criminal acts) and **must suspend its actions** when these bodies initiate an investigation.

New EU AML and CFT package of rules, 30 of May 2024

The EU's new anti-money laundering (AML) and countering the financing of terrorism (CFT) legislative package consists of the following rules:

1. Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing:

- Includes **requirements for obliged entities**, mainly financial and credit institutions and designated non-financial businesses and professions (e.g. lawyers and accountants).
- **Extends the list of obliged entities to:**
  - **Dealers in luxury cars, aircraft, yachts and cultural goods** (such as works of art).
  - **Crypto-asset service providers.**
  - **Crowdfunding platforms.**
  - **Mortgage and consumer credit intermediaries** that do not qualify as financial institutions.
  - **Investment migration operators working** on behalf of third-country nationals in order to obtain a residence permit in the EU.
  - **Professional football clubs and agents**. However, given that the sector and its risk are subject to wide variations, Member States will have the flexibility to remove them from the list if they represent a low risk.
- It requires obliged entities **to have a "compliance manager"** and a **"compliance officer"** for the prevention of money laundering.
- It requires **obliged entities** to apply **enhanced due diligence measures to occasional transactions** and **business relationships** involving high-risk third countries.

New legislation

MOLINS Compliance

2. **Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (AMLA)**

- A new Anti-Money Laundering Authority (AMLA) is established to improve the **supervision** of the fight against money laundering and terrorist financing in the EU and to support cooperation between FIUs. It will have the following functions:
  - **Coordination and harmonisation function:** it will issue technical guides to facilitate cooperation and exchange of information between the FIUs of the Member States; it will improve the electronic systems used by the FIUs and Europol for the exchange and verification of information.
  - **Supervisory function:** it will directly supervise obliged entities, especially those with a high risk of money laundering; it will act at the request of Member States' financial intelligence units or on its own initiative if there is a Union interest in supervising certain entities.
- The ALBC will be **based in Frankfurt** and will start operating in **mid-2025.**

This Regulation will apply from **1 July 2025**, with the exception of some of its provisions which already apply from **26 June 2024** or will apply from **31 December 2025.**

3. **Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849Text with EEA relevance.**

- This Directive sets out **specific measures** for **sectors exposed to money laundering at national level**. These measures include requirements for the registration, identification and control of senior management and beneficial owners of obliged entities.
- It expands the information to be included in these central registers, covering security issues and crypto-asset accounts.
- The **centralised automated mechanisms shall be interconnected via the bank account registers interconnection system** (BARIS), to be developed and operated by the Commission by 10 July 2029. The Anti-Money Laundering Authority (AMLA), state financial intelligence units and national AML/CFT supervisory authorities will have direct access to BARIS.

The deadline for transposition of this Directive is **10 July 2027.**

4. **Directive (EU) 2024/1654 of the European Parliament and of the Council of 31 May 2024 amending Directive (EU) 2019/1153 as regards access by competent authorities to centralised bank account registries through the interconnection system and technical measures to facilitate the use of transaction records:**

- This Directive aims to ensure that national law enforcement authorities also have access to centralised records of bank accounts through the single access point.

The deadline for transposition of this Directive is **10 July 2027.**

New legislation

MOLINS Compliance

Regulation of the European Parliament and of the Council laying down harmonised rules in the field of artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union (Regulation of the European Parliament and of the Council on Artificial Intelligence - AIA).

The **AI Regulation** seeks to regulate the **uses of Artificial Intelligence** in order to limit the risks arising from them.

Its scope extends to:

- **Providers** of AI systems that are put into service or placed on the market within the EU or used in the EU, irrespective of their origin;
- **Users** of such systems located in the EU, where users are considered to be those who operate such systems, and not those concerned.
- **Providers and users** of AI systems located in a third country, where the output produced by the system is used in the Union;

Among other issues, this Regulation **classifies AI according to the level of risk:**

- **Unacceptable risk (prohibited AI):** this includes AI systems that distort human behavior, social assessment and classification, and real-time remote biometric identification (in public spaces).
- **High risk (AI allowed with limitations):** covers AI applicable to education and vocational training, essential infrastructure (e.g. transport), recruitment, workforce management and access to self-employment, access to and enjoyment of essential private services and public services and benefits, law enforcement, migration management, asylum and border control, and the administration of justice and democratic processes.

For **high risk systems**, several obligations are established: to have a risk management system, to establish governance and management of training and test data, to have updated technical documentation demonstrating compliance with the requirements, to have records of system activity, among others.

- **Limited risk (AI allowed with fewer limitations):** the obligation to ensure human supervision and notification of users when interacting with AI systems is established.
- **Minimal risk (permitted AI):** includes those AI systems that do not fall into the above categories.

One of the key institutions in the implementation and oversight of this regulation is the **EU Office for Artificial Intelligence**, which will be responsible for **coordinating regulatory activities and oversight at the European level**, ensuring **consistent application across all member states.** In addition, it will also provide technical and operational guidance to AI developers and users, manage AI-related incident reports, among other functions.

Furthermore, the AI Regulation creates the **European AI Council**, with advisory and assistance functions to Member States to ensure its consistent application. At national level, Member States are required to designate **at least one national market surveillance authority and one notifying authority.**

In this regard, and in view of the **increasing use of AI systems** in entities across all sectors, it is crucial to comply with regulatory standards by protocolising management and control measures.

By adopting **measures to ensure security and ethics** in the application of AI, organisations can proactively demonstrate their commitment to regulation and social responsibility. This not only helps to avoid sanctions, but also increases the confidence of third parties such as customers and business partners.

The Regulation will enter into force on **1 August 2024** and will apply from **1 August 2026**, with some exceptions.

Case law

- Decision 179/2023, of 11 December 2023 of the Second Chamber of the Constitutional Court
- Decision of the Supreme Court (Social Chamber) 225/2024, of 6 February 2024
- Decision of the Supreme Court (Criminal Chamber) 165/2024, of 22 February 2024
- Decision of the Supreme Court (Criminal Chamber) 217/2024, of 7 March 2024
- Decision of the Supreme Court (Criminal Chamber) 298/2024, of 8 April 2024
- Decision of the Supreme Court (Social Division) 874/2024, of 5 June 2024

Decision 179/2023, of 11 December 2023 of the Second Chamber of the Constitutional Court

In this decision, the Constitutional Court rules on the appeal for amparo brought by Banco Santander, S.A. against the resolutions of the Council of Ministers which sanctioned the entity for **failure to report suspicious money laundering transactions**. That sanction arose following an **inspection by SEPBLAC of Banco Popular, S.A.**, which was later **absorbed by Banco Santander.** A fine of 1.056.000 euros was imposed for a very serious infringement of Article 51.1.a) of Law 10/2010 on the prevention of money laundering and terrorist financing (AML/CFT), due to **the failure to report certain suspicious transactions.**

Banco Santander argued that the **sanction violated the principle of the legality of penalties** under Article 25.1 of the Spanish Constitution (EC), in its aspects of **culpability and personality of the penalty.** It argued that there was no continuity between Banco Popular, S.A. and Banco Santander, as well as changes in the procedures for the prevention of money laundering after the absorption and the absence of benefit derived from the infringing conduct. However, the **Constitutional Court** holds that, according to the consolidated case law of the Supreme Court and the Court of Justice of the European Union, in cases of M&A, **liability for administrative infringements** is **transferred** when there is **"substantial economic identity**", thus ensuring the **continuity of liabilities as the same economic activity persists under a new legal ownership.**

The Court concludes that the **sanctioning decision does not infringe the principles of guilt and personality of the penalty** in Article 25.1 EC. The "substantial economic identity" between Banco Popular, S.A. and Banco Santander, S.A. justifies the transfer of liability for infringement, and the **absence of profit does not eliminate that liability**. Consequently, the application for amparo brought by Banco Santander is dismissed, upholding the validity of the sanction imposed.

Decision of the Supreme Court (Social Chamber) 225/2024, of 6 February 2024

In this decision, the **Supreme Court** addresses the nullity of the guidelines established by a company on the use of digital devices provided to employees, due to the **lack of participation of workers' representatives in the drafting of the policy on the use of digital devices** (IT or ICT policies).

This decision is based on the **failure to comply with article 87.3 of the Organic Law on Data Protection (LOPD, for its acronym in Spanish)**, which requires **the participation of workers' representatives in the creation of policies related to the use of information and communication technologies.** The company argued that the nullity of the instructions **violated its right to corporate control** (article 20.3 of the Workers' Statute) and argued that the challenged instructions were only a reminder of policies prior to the entry into force of article 87.3 of the LOPD in 2018.

However, the Supreme Court concluded that, although the obligation to include workers' representatives in the creation of such policies (art. 87.3 LOPD) does not have retroactive effect, the guidelines represented a fundamental change in the rules of use and their control, confirming their nullity.

Decision of the Supreme Court (Criminal Chamber) 165/2024, of 22 February 2024

In this decision, the Supreme Court addressed an appeal in cassation against a conviction for **the offence of asset stripping.**

The appellants, among other issues, argued that **the offence of asset stripping** was configured as a **special offence of its own**, whose perpetrator must be the debtor, and that they **could not be convicted as such without a direct accusation against the legal person.**

The Supreme Court rejected this argument, stating that **Article 31 of the Criminal Code extends liability to those who carry out the acts of execution as de facto administrators of a legal person,** even if they do not meet the conditions required to be active subjects of the offence.

The decision concluded that both appellants exercised **effective control over the companies involved and orchestrated the sale of assets to avoid paying labour debts**, which justified their conviction.

Decision of the Supreme Court (Criminal Chamber) 217/2024, of 7 March 2024

This Supreme Court decision deals with the case of tax fraud and criminal liability of a commercial company. The facts are related to the **tax activity of the company and its administrator**, who was convicted of several offences of VAT and corporate tax fraud in 2011 and 2012.

Specifically, as regards the criminal liability of the legal entity, the Supreme Court confirmed the imposition of **significant fines and the loss of tax benefits for the company**, emphasising that the company was **used to commit the tax offences.** Finally, the Supreme Court clarified that the penalties imposed on both the natural person and the legal entity, despite the arguments of the defense regarding a possible doubling of the financial burden, were absolutely **proportional to the gravity of the facts**.

Decision of the Supreme Court (Criminal Chamber) 298/2024, of 8 April 2024

The Supreme Court decision, STS 298/2024, resolves an appeal in cassation brought by several of those convicted of offences against the Public Treasury and forgery of documents. The case mainly involves three legal entities and their respective owners.

The High Court holds that the **companies in question facilitated tax fraud by means of simulated contracts and fictitious payments**. In turn, it discusses the application of article 31 *bis* of the Criminal Code, which **extends criminal liability to legal persons when their managers or employees commit offences for the benefit of the entity.** In this case, it was concluded that the companies had indeed been **used to conceal income and facilitate such fraud.**

However, the Supreme Court decided to acquit the three legal persons, arguing that the **existence of a direct or indirect benefit derived from the offence of tax fraud** committed by the respective natural persons involved had **not been proven**.

Among others, the Supreme Court clarifies that the tax fraud committed by one of the natural persons not only did **not generate additional benefits for these companies**, but rather **harmed them**. Furthermore, it emphasises that the double conviction of the companies and their directors, in the present case, would violate the **principle of *non bis in idem*.**

Decision of the Supreme Court (Social Division) 874/2024, of 5 June 2024

In the present decision, the Supreme Court rules on the disciplinary dismissal of a worker who was caught with unpaid goods in her purse after the anti-theft alarm went off.

The **search of the bag** was carried out by a **security guard without the presence of a legal representative of the workers or another worker**, in violation of Article 18 of the Workers' Statute (ET, for its acronym in Spanish).

The failure to observe these legal safeguards led the High Court of Justice of Andalucía to **declare the dismissal null and void**, since the search, without the proper safeguards, **lacked probative value.**

Thus, in the present decision, **the Supreme Court confirms that article 18 of the ET requires the presence of a legal representative of the workers or another worker to ensure the objectivity and effectiveness of the evidence.**

The absence of this guarantee implies that any evidence obtained in the register cannot be used to justify dismissal. Furthermore, it is stressed that compliance with these rules is essential **to protect the rights of workers and to maintain the integrity of the disciplinary process.**

In this case, the criminal liability of the legal entity was focused on its failure to ensure that the search of the employee's handbag was carried out in accordance with the legal guarantees, which led to the violation of the employee's rights and the nullity of the dismissal. Finally, **the company was ordered to reinstate the worker and to pay her lost wages.**

Other agreements and sanctioning resolutions on Compliance

MOLINS
Compliance

- 23.7 million euros stolen through artificial intelligence fraud.
- AEPD fines Spanish company 365,000 euros for making its employees sign in with fingerprints
- Santander, BBVA and Telefónica dismiss 590 workers due to co-worker allegations
- 32 million fine for Amazon for going too far in monitoring its employees
- More than 16 million euros in fines for privacy infringements in 2023
- Adidas managers in China investigated in alleged corruption case
- BBVA fined 200,000 euros for including a customer in a debt collection file without prior notice

Other agreements and sanctioning resolutions on Compliance

MOLINS Compliance

23.7 million euros stolen through artificial intelligence fraud

An **employee of a financial firm** in Hong Kong transferred **23.7 million euros to what he believed was his company's UK subsidiary,** duped by a sophisticated **artificial intelligence scam.**

The fraudsters used **deepfake** technology to pretend to be the CFO and other colleagues during a video call, convincing the employee of the legitimacy of the transfer request. Hong Kong police have made six arrests in connection with the case, highlighting concerns about the increase in this type of fraud with the advancement of generative artificial intelligence technologies.

AEPD fines Spanish company 365,000 euros for making its employees sign in with fingerprints

The **Spanish Data Protection Agency has fined a Spanish company 365.000 euros** for **requesting employees' fingerprints** for clocking in.

The company in question collected **biometric data from employees and stored it in the employee portal,** without previously informing them of this fact.

The company claimed that it had been **properly informed of the data processing.** However, it was found that **the information provided was not sufficient and that the deletion of the fingerprint after capture was not guaranteed** and the employee's identification data was stored.

Santander, BBVA and Telefónica dismiss 590 workers due to co-worker allegations

During 2023, **Santander, BBVA and Telefónica dismissed a total of 590 employees due to complaints made by colleagues** through internal whistleblowing channels.

Specifically, Santander dismissed 366 employees, while BBVA dismissed 115 and Telefónica 109.

The processing of these situations through the whistleblowing channel allows the **corresponding investigation of the facts to be carried out through the established procedure**, preserving the **guarantees and rights of the whistleblower**.

32 million fine for Amazon for going too far in monitoring its employees

The **French Data Protection Agency** (CNIL, for its acronym in French) has fined Amazon France Logistique **32 million euros for a labour monitoring system deemed "excessively intrusive".**

This system, which involves scanners to measure employee productivity in real time, has been criticised for **violating the right to privacy and the principles of the French Labour Code.**

The CNIL also questions the **retention of detailed data on workers activity and the lack of adequate information on the video surveillance system.** Amazon, for its part, has defended these methods as industry standards to ensure quality and labour efficiency, announcing its intention to appeal the decision.

Adidas managers in China investigated in alleged corruption case

Several Adidas employees in China publicly accused company officials of **fraud in an alleged case of large-scale bribery.**

Specifically, the allegation is based on several **screenshots** alleging that **managers received bribes and other physical gifts**, such as real estate, from **external service providers in order to secure a contract between Adidas and the service providers.**

Other agreements and sanctioning resolutions on Compliance

MOLINS
Compliance

More than 16 million euros in fines for privacy infringements in 2023

In 2023, the **Spanish Data Protection Agency (AEPD) imposed more than 16 million euros in fines** for various privacy infringements.

The **highest penalty** of 6 million euros **was imposed on Endesa** for a **security breach** that compromised the data of millions of individuals. This incident underlines the critical importance of maintaining rigorous data security measures. In addition, fines in 2024 are expected to be less frequent but higher, reflecting a trend towards **more severe enforcement of the General Data Protection Regulation (GDPR) in Spain.**

Companies face significant challenges in adequately implementing data protection and security measures, particularly in sectors such as financial services and telecommunications, where **the risks of non-compliance are higher due to the handling of sensitive data and the need for robust security safeguards.**

BBVA fined 200,000 euros for including a customer in a debt collection file without prior notice

The **Spanish Data Protection Agency imposed a fine of 200,000 euros on BBVA** for requesting the **inclusion of a customer's personal data in a debtors' file** without prior notification.

In the present case, the customer in question was **included on this list for non-payment** of a **credit card** as a cardholder. The problem lies in the fact that he was not notified of this inclusion because the address provided was inaccurate, causing him serious damage.

These facts constitute a **breach of Article 5(1)(d) of the General Data Protection Regulation,** which requires the accuracy of the personal data collected, updating them where necessary.

Guides, institutional resolutions and reports of interest

MOLINS Compliance

- ISO 42001, Artificial Intelligence Management Systems
- ISO 45004, Health and Safety at Work. Occupational Health and Safety Management Systems. Performance evaluation
- UNE 15713, Secure Destruction of Confidential and Sensitive Material
- UNE 171380, Continuous indoor CO2 measurement for health prevention and improvement of well-being
- UNE-ISO 10010, Quality management. Guidance for understanding, evaluating and improving the quality culture in the organization
- UNE-ISO 10017, Quality Management. Guidance on statistical techniques for the ISO 9001:2015 Standard
- UNE-ISO 53800, Guidelines for the promotion and implementation of gender equality and women empowerment
- The CNMC's "Guide for quantifying harm from competition law infringements"
- Opinion 0077/2023 of the AEPD on the feasibility of processing personal data contained in communications received through the Internal Information System (SII) for purposes other than those provided for by Law 2/2023
- Resolution of the most frequently asked questions on Law 2/2023, of 20 February, regulating the protection of persons who report regulatory and anti-corruption offences by the Anti-Fraud Office of Catalonia

Guides, institutional resolutions and reports of interest

MOLINS Compliance

ISO 42001, Artificial Intelligence Management Systems

In response to **the rise of Artificial Intelligence** (AI) and the challenges it presents, ISO and IEC have developed ISO/IEC 42001:2023.

This initiative responds to the need to properly **manage the risks and maximise the benefits** that AI and machine learning can bring to society and the economy, such as **advanced data interpretation and remote diagnostics.**

ISO/IEC 42001:2023, applicable to any company, aims to ensure responsible **development and use of AI**, promoting ethical principles such as fairness and respect for privacy.

This ISO standard helps organisations to identify and mitigate risks, ensuring legal compliance and data protection. It also prioritises human well-being and **safety in the design and deployment** of IA systems, thus contributing to business **resilience and sustainability.**

ISO 45004, Health and Safety at Work. Occupational Health and Safety Management Systems. Performance evaluation

ISO 45004:2024 provides guidance to organisations of all types on **how to proceed in the following aspects:**

- Establishment of **processes for monitoring, measuring, analysing and evaluating occupational health and safety** (OSH) **performance**.
- **Developing relevant indicators** to measure the success of their OSH initiatives.
- **Determination of compliance with OSH outcomes and objectives**.
- Identification of **areas for improvement and implementation of measures to improve** the organisation's efficiency and productivity.

The implementation of ISO 45004:2024 enables you to **improve OSH performance and demonstrate the effectiveness of your management systems**, provide greater confidence to stakeholders, identify and address OSH risks proactively, and reduce occupational accidents and illnesses.

UNE 15713, Secure Destruction of Confidential and Sensitive Material

The **UNE 15713:2024 standard** establishes **requirements and recommendations** for **the safe physical destruction of confidential and sensitive material** in any company that processes this type of material.

This standard regulates different situations, covering aspects such as the use of mobile equipment at the place of use and the use of equipment by the data controller.

Among the issues addressed in the standard are the **recording of the process** from collection to **destruction, outsourcing, personnel confidentiality agreements, the collection and transport of confidential and sensitive material**, and the **storage and preservation** of such material at the destruction facility.

UNE 171380, Continuous indoor CO2 measurement for health prevention and improvement of well-being

In view of the need to **complement and improve the requirements established by quality standards and current legislation**, the new standard UNE 171380:2024 has been developed.

This standard is applicable to all **buildings for collective use**, including both new and existing buildings.

This standard covers the **requirements to be met by the measuring equipment**, the project for its implementation according to the typology and uses of the building, the **management of the data obtained**, as well as the establishment of the **CO2 concentration thresholds** foreseen for air quality and the **procedures for auditing** them.

Guides, institutional resolutions and reports of interest

MOLINS Compliance

UNE-ISO 10010, Quality management. Guidance for understanding, evaluating and improving the quality culture in the organisation

The **UNE-ISO 10010:2024** standard establishes recommendations on the **evaluation, development and improvement of quality management in an organisation.**

This standard covers the **fundamental concepts and general principles** of quality management, as well as the **specific commitment of the people** who make up the organisation and the need for their **leadership** in this process.

UNE-ISO 10017, Quality Management. Guidance on statistical techniques for the ISO 9001:2015 Standard

The **new UNE-ISO 10017:2024** provides **guidelines for organisations to manage their quality through statistical control of their processes**. This control includes the selection of statistical techniques that promote the development, implementation, maintenance and improvement of a quality management system, in accordance with the provisions of UNE-EN ISO 9001:2015.

UNE-ISO 53800, Guidelines for the promotion and implementation of gender equality and women empowerment

Persistent **gender inequalities within organisations** reflect the need to develop regulations that eradicate the structural discrimination existing in today's society. In view of this situation, the **UNE-ISO 53800:2024 standard provides guidelines, definitions, procedures and tools** for **public and private organisations** aimed at **promoting and guiding** them towards achieving gender equality both within and outside the organisation.

The CNMC's "Guide for quantifying harm from competition law infringements"

The new **Guide to the quantification of damages for competition law infringements, published by the National Commission for Markets and Competition (CNMC),** sets out a detailed framework for calculating the economic damages caused by violations of competition rules in Spain. This guide aims to **provide courts and affected parties with precise tools and clear methodologies to determine the extent of damages suffered**, especially in cases of anti-competitive practices such as restrictive agreements or abuses of dominance.

In its new guidelines, the CNMC emphasises the importance of **adopting robust and consistent approaches to the quantification of damages**, including methods such as benchmarking, econometric modelling and the evaluation of financial and commercial data. It also stresses the need to properly consider the economic and sectoral context in which infringements occurred, ensuring that compensation accurately reflects the harm caused to consumers and other parties affected by anti-competitive practices.

Guides, institutional resolutions and reports of interest

MOLINS Compliance

Opinion 0077/2023 of the AEPD on the feasibility of processing personal data contained in communications received through the Internal Information System (SII) for purposes other than those provided for by Law 2/2023

The AEPD, in its Opinion 77/2023, assesses the possibility of **processing personal data** received through the Internal Information System (SII, for its acronym in Spanish) **for purposes other than those established by Law 2/2023**, which protects whistleblowers.

Thus, for **entities bound by this law**, the **processing is justified** by compliance with **legal obligations** (**Article 6.1.c)** of the GDPR), while for those not subject to it, the processing could be based on the **legitimate interest of the data controller,** always protecting fundamental rights.

Finally, it should be noted that the Agency places particular emphasis on the need to adhere to **the purpose limitation principle**, ensuring that data are collected for **specified, explicit and legitimate purposes (Article 5.1.b) of the GDPR**, assessing the **compatibility of any new processing** with the **reasonable expectations of data subjects** and always ensuring **adequate protection of personal data** as established by the current regulations and data protection principles.

Resolution of the most frequently asked questions on Law 2/2023, of 20 February, regulating the protection of persons who report regulatory and anti-corruption offences by the Anti-Fraud Office of Catalonia

The **Anti-Fraud Office of Catalonia**, as the competent autonomous authority for the protection of whistleblowers, continuously updates its **compendium of answers to the most frequent doubts that have been raised in relation to the interpretation of Law 2/2023**, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption.

Among many other questions, the following **stand out due to their practical impact**:

- What obligations does the entry into force of Law 2/2023 give rise to?
- Do persons who report an offence falling within the scope of Law 2/2023 through the internal channel of a non-obliged entity enjoy protection vis-à-vis this entity?
- How should the Anti-Fraud Office be notified of the appointment and dismissal of the person(s) responsible for the Internal Information System? In this respect, it is important to point out that the Anti-Fraud Office of Catalonia **has updated the form** for notifying the appointment and dismissal of the natural person or persons who form part of the collegiate body designated as the person(s) responsible for the internal information system. This form is **available on its website.**

Compliance Department publications (January - July 2024)

MOLINS
Compliance

- Current developments in Compliance: the publication of the UNE 19603 on Compliance Management Systems regarding free competition.
- The deadline for adapting the use of cookies has expired
- The new Foreign Extortion Prevention Act
- Regarding the delicate balance between Equality and Compliance policies in relation to Protocols against Mobbing and Sexual Harassment
- Is there a succession of administrative liability in M&A? Brief commentary on Judgement 179/2023 of 11 December 2023 of the Second Chamber of the Constitutional Court
- The challenge of corporate sustainability reporting for organizations in relation to the new report “Supporting ESG reporting standards”
- More than 80% of Catalan companies fail to comply with Law 2/2023
- Spain continues its fight against corruption: A detailed analysis of judicial progress in 2023
- Three notes on the criminal liability of legal persons: Judgment no. 298/2024 of 8 April 2024
- Progress in the Implementation of the Independent Whistleblower Protection Authority
- Can personal data contained in communications received through the Internal Information System (IIS) be processed for purposes other than those provided for in Law 2/2023?

MOLINS

Defensa Penal **Compliance**

Barcelona Diagonal 399, Planta 1 08008 | Tel. 93 415 22 44

Madrid José Abascal, 56 Planta 6 28003 | Tel. 91 310 30 08

www.molins.eu | compliance@molins.eu