MOLINS

Defensa Penal **Compliance**

Compliance Newsletter Year Review

2024

Table of contents

Introduction

Compliance has positioned itself as a key element in guaranteeing the solidity and ethics of organisations in today's complex and dynamic regulatory framework. In this context, **continuous updating is not only a duty**, but **an indispensable strategic necessity** to address current challenges and anticipate those to come.

During the past 2024 there have been **important regulatory and jurisprudential developments in the field of Compliance**, both at national and international level, which must be taken into consideration. In this regard, new developments have been observed such as:

- The long-awaited **creation at state level of an Independent Whistleblower Protection Authority** (or, at the very least, the Statute by which this Authority should be governed when it is materially constituted);
- **Regulation at European level on Artificial Intelligence, cybersecurity and cyber-resilience**;
- **New obligations on sustainability** and on the **protection of LGTBI rights in the workplace**;
- Or, even, **new jurisprudential trends in relation to the burden of proof of the design, implementation and effectiveness of Compliance Systems**, as well as their relevance with regard to such significant criminal offences as **fraud against the Spanish Public Treasury**.

In this context, the Compliance Department of Molins Defensa Penal has prepared this Newsletter as a review of the main milestones in the field of Compliance in 2024. Its content is structured as follows:

- A detailed analysis of the most **relevant legislative developments** that impact on the configuration and improvement of Compliance Systems will be carried out.
- This will be followed by a presentation of **relevant rulings on Compliance** issued by the Spanish Supreme Court, the Constitutional Court and the National High Court.
- Next, other significant **agreements and sanctioning resolutions** in the field of Compliance will be presented.
- It will also include a brief presentation of **guides, institutional resolutions and recent reports** of particular interest.
- Finally, this Newsletter will conclude with a summary of the **Compliance Department's publications** for the year 2024.

New legislation

MOLINS Compliance

- Corporate Sustainability Due Diligence Directive (CSDDD) No. 2022/2464.
- Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER).
- New Foreign Extortion Prevention Act (FEPA).
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2).
- Establishment of the Independent Whistleblower Protection Authority.
- New EU AML/CFT package, 30 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 31 May 2024 establishing a European Anti-Money Laundering and Terrorist Financing Authority (AMLA).
  - Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Directive and (EU) 2019/1937 and amending and repealing Directive (EU) 2015/849.
  - Directive (EU) 2024/1654 of 31 May 2024 amending Directive (EU) 2019/1153 as regards access by competent authorities to centralised records of bank accounts through the Interconnection System and technical measures to facilitate the use of trade repositories.
- Regulation of the European Parliament and of the Council on Artificial Intelligence (AIA - Artificial Intelligence Act).
- Royal Decree 1026/2024, which develops measures for equality and non-discrimination of LGTBI people in companies.
- Draft Law on Corporate Reporting on Sustainability for the disclosure of companies' contribution to environmental, social and governance issues.

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 requires organisations 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 Pact** and are based on the **European Sustainability Reporting Standards**.

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

The **control of compliance with the provisions of the CSDDD** shall be carried out by the relevant specialised body of the public administration which shall have the following powers:

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

Which self-regulatory standards can organisations choose to comply with in order to facilitate compliance with these obligations? Among others, with the following:

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

This Directive was published in the Official Journal of the European Union (hereinafter, OJEU) on **26 July 2024** and is **pending transposition into Spanish law.**

Directive (EU) 2022/2557 of the European Parliament and of the Council 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, response, recovery measures**, etc.
- **Background checks**.
- **Incident reporting**.

The CER Directive applies to **critical entities, which must be identified by 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 expired on **17 October 2024**, and its transposition into Spanish law is pending.

New legislation

MOLINS
Compliance

The new 'Foreign Extortion Prevention Act' (FEPA)

The **FEPA** complements the Foreign Corrupt Practices Act (FCPA) and establishes, for the first time, **criminal liability for foreign officials** who solicit or accept bribes from people 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 or 3 times the value of the bribe, imprisonment for up to 15 years**, or even both.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure 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 sector; drinking water; waste water; digital infrastructure; ICT service management (B2B); public administration entities (excluding judiciary, parliaments and central banks); and space.
- **Other critical sectors**: postal services; waste management; manufacture, production and distribution of chemicals and chemical mixtures; food production, processing and distribution; manufacturing; digital service providers; and research.

The deadline for transposition of this Directive expired on **17 October 2024**, and its transposition into Spanish law is pending.

New legislation

MOLINS Compliance

Creation of the Independent Authority for the Protection of Whistleblowers

On October 31, Royal Decree 1101/2024, dated October 29, was published in the Spanish Official State Gazette, approving the Statute of the Independent **Authority for the Protection of Whistleblowers (A.A.I.).**

The A.A.I. is a state entity with **autonomy and functional independence** whose objective is to comply with the **mandate of Law 2/2023.**

The **functions** of the A.A.I. are, among others, the following:

- **Processing of information and communications** carried out through the external channel of the A.A.I. itself.
- Adoption of **protection and support** measures for informants.
- **To report on the preliminary drafts and projects of general** provisions that affect the Authority's area of competence.
- **Initiation, instruction and resolution of sanctioning procedures**.
- Preparation of **circulars and recommendations** establishing the criteria and appropriate practices for the correct operation of the Authority.
- Establish **collaboration relationships with other similar authorities** (e.g.: Anti-Fraud Office of Catalonia).
- To prepare 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 non-compliances in terms of whistleblower protection** of **Spanish Law 2/2023**. In spite of this, the A.A.I. cannot exercise the functions of judges or prosecutors (it cannot investigate facts of a criminal nature) and must **suspend its actions** when such bodies initiate an investigation.

The Draft Royal Decree provides for the **creation of an external channel for complaints, universally** accessible and open to any interested person.

Finally, it is interesting to note the creation of a **collegiate body of a multidisciplinary nature**, called the **Consultative Commission for Whistleblower Protection**, with representation from the Court of Auditors, the State Attorney General's Office, the CNMC and CNMV, etc., with **advisory functions** to the Presidency of the A.A.I.

New European Union AML-FT package, 30 May 2024

The new European Union package of measures for the prevention of Money Laundering and Terrorist Financing 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).
- **Expands the list of obligated entities** to:
  - **Dealers in luxury cars, aircraft, yachts and cultural property**.
  - **Cryptoasset service providers**.
  - **Crowdfunding platforms**.
  - **Mortgage and consumer credit intermediaries** that are not considered financial institutions.
  - **Investment migration operators** working on behalf of third country nationals in order to obtain a residence permit in the EU.
  - **Professional soccer 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 pose a low risk.
- It requires obliged entities **to have a "chief compliance officer" 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 31 May 2024, establishing a European Anti-Money Laundering and Terrorist Financing Authority (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 harmonization function**: it will issue technical guides to facilitate cooperation and exchange of information between the Financial Intelligence Unities (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 the financial intelligence units of the Member States or on its own initiative if there is a Union interest in supervising certain entities.
- The AMLA will be **based in Frankfurt** and will start operating in **mid-2025.**

This Regulation will apply as of **July 1, 2025**, except for some of its provisions which are already applicable as of **June 26, 2024** or will be applicable as of **December 31, 2025**.

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

- It establishes **specific measures** for **sectors exposed to money laundering at national level**. These measures include requirements for registration, identification and control of senior management and beneficial owners of obliged entities.
- **It expands the information** to be included in these central registries**,** covering **security issues and cryptoasset accounts.**
- **The automated centralized mechanisms will be interconnected through the Bank Account Record Interconnection System** (BARIS), to be developed and managed by the Commission by July 10, 2029. The Anti-Money Laundering Authority (AMLA), state financial intelligence units and national AML/FT supervisory authorities will have direct access to BARIS.

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

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

- It aims to ensure that national law enforcement authorities also have access to centralized bank account records 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 harmonized 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, *for Artificial Intelligence Act*-).

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

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, regardless of their origin;
- **Users** of these that are located in the EU, considering users to be those who operate such systems, and not those concerned.
- **Providers and users** of AI systems located in a third country, when the systems produce results that are used in the EU.

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

- **Unacceptable risk (prohibited AI)**: it includes AI systems that distort human behaviors, social assessment and ranking, and real-time remote biometric identification (in public spaces).
- **High risk (AI allowed with limitations):** it covers AI applicable to education and vocational training, essential infrastructure (e.g., transportation), personnel selection, labor 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 (AI allowed)**: includes those AI systems that do not fall into the above categories.

One of the key institutions in the implementation and supervision of this regulation is the **EU Office for Artificial Intelligence**, created by the European Commission, which will be responsible for **coordinating regulatory activities and supervision at the European level, ensuring consistent application in 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.

On the other hand, the **IA Regulation creates a European IA Council**, with **advisory and assistance** functions to the Member States to ensure consistent application.

At the 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 in all sectors, it is crucial to comply with regulatory standards by protocolizing management and control measures.

Adopting **measures to ensure security and ethics** in the application of AI allows organizations to 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 entered into force on **August 1, 2024** and will be applicable on **August 1, 2026**, with some exceptions.

New legislation

MOLINS Compliance

Royal Decree 1026/2024, which develops measures for equality and non-discrimination of LGTBI people in companies.

Last October 8, **Royal Decree 1026/2024** was published, which strengthens the measures aimed at guaranteeing **equality and non-discrimination of LGTBI people** in the **workplace** (hereinafter, RD 1026/2024). This regulation introduces the **obligation** for companies with **more than fifty (50) employees** to implement a **minimum set of measures and resources** established in its annexes, with the aim of promoting **real and effective equality in the professional environment with respect to LGTBI people**.

Specifically, **the measures provided for in RD 1026/2024** cover:

- **Annex I**: Includes equal treatment and non-discrimination clauses, as well as specific actions to guarantee access to employment, professional promotion and training for LGTBI people. It also promotes awareness in diverse and inclusive work environments, the establishment of specific leave and social benefits, as well as adjustments in disciplinary regimes that reinforce protection against discriminatory behavior.
- **Annex II**: Establishes a model protocol against harassment and violence, with provisions ranging from a statement of principles to the definition of procedural safeguards and effective resolution mechanisms. It should be noted that, although many companies already have generic protocols, RD 1026/2024 makes it mandatory to update them to include the specific measures it contemplates.

In addition, **companies obliged to negotiate planned measures regulating their working conditions through collective bargaining agreements or company agreements, as well as those without a collective bargaining agreement, but with legal representation of workers, must set up a negotiating committee within a maximum period of three (3) months from the entry into force** of RD 1026/2024 **(January 10, 2025).**

For **companies without legal representation, the term is extended to 6 months. If an agreement is not reached within 3 months from the beginning of the negotiation**, companies with more than 50 workers **will apply the measures established in the regulation** until others are agreed upon through negotiation.

In line with this legislative evolution, **the XXI General Chemical Industry Agreement** (hereinafter CGIQ), whose pre-agreement was signed the day after the publication of RD 1026/2024, **is positioned as the first agreement to incorporate these specific measures.**

This agreement adopts a **cross-cutting approach** to equality and non-discrimination of LGTBI people, developing and even **expanding some of the measures contemplated in RD 1026/2024**. For example, in the training plans, it is included that the courses aimed at people involved in selection processes or with roles of responsibility incorporate additional aspects that the Royal Decree does not foresee. Likewise, the CGIQ agrees a **protocol against harassment and violence** that integrates specific measures aimed at the protection of LGTBI people.

In this regard, the **protocol provided for in the CGIQ stands out for establishing a detailed procedure**, which includes **previous phases of rapid mediation and formal processes**, in addition to guaranteeing the optional participation of workers' representatives. However, this protocol establishes the **submission of complaints or denunciations directly to "the Heads of Human Resources**", leaving aside the provision of RD 1026/2024 to **respect the mechanisms established by Law 2/2023**.

Draft Corporate Sustainability Reporting Bill for the disclosure of companies' contribution to environmental, social and governance issues.

The **Corporate Sustainability Reporting Bill** aims to improve the **framework for the presentation and verification** of sustainability information by companies. This draft law, **approved by the Council of Ministers on October 29, 2024, amends the Commercial Code, the Capital Companies Act and the Accounts Auditing Act**.

Among the **main new features** is the obligation for companies to include in their reports **detailed information** on their impact on **environmental, social and governance issues**, as well as the effects of these factors on their performance and financial situation.

In addition**, it establishes the creation of a single presentation format at European level** for sustainability reports, in an **electronic format** that will facilitate the comparability and **accessibility of the information** between the different Member States. The law provides for a **staggered timetable** for its entry into force, allowing entities to **progressively adapt** their Compliance management systems to the new European regulations and standards.

Case law

- Decision 179/2023 of December 11 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 165/2024, of 22 February, 2024.
- Decision of the Supreme Court 217/2024, of 7 March, 2024.
- Decision of the Supreme Court 298/2024, of 8 April, 2024.
- Decision of the Supreme Court 874/2024, of 5 June, 2024.
- Decision of the National Audience Court, Criminal Chamber, of 12 July, 2024.
- Decision of the Provincial Court of Mallorca 559/2024, of 16 December, 2024.

Case law

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 constitutional protection filed by Banco Santander, S.A., against the resolutions of the Council of Ministers that sanctioned the entity for **the lack of communication of suspicious transactions of money laundering**. This sanction originated after an **inspection by SEPBLAC of Banco Popular, S.A.**, an entity that 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 (LPBC), **due to the failure to report certain suspicious transactions.**

Banco Santander alleged that the **sanction violated the principle of legality of the sanction** in Article 25.1 of the Spanish Constitution (EC), in its aspects of **guilt 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 takeover and the absence of benefit derived from the infringing conduct. However, the **Constitutional Court** held that, according to the consolidated case law of the Supreme Court and the Court of Justice of the European Union, in cases of merger by absorption, **liability for administrative infringements is transferred when there is a "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 resolution does not violate the principles of culpability and personality of the penalty** of 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 such liability**. Consequently, the appeal filed by Banco Santander is dismissed, ratifying the validity of the sanction imposed.

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

The **Supreme Court** addresses in this decision 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 TIC policies).**

This ruling is based on the **failure to comply with article 87.3 of the Organic Law on Data Protection (LOPD),** 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 effects, 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 the present Ruling, the Supreme Court addresses the appeal filed against a conviction for the crime of **fraudulent conveyance**.

The appellants, among other issues, argued that the **crime of fraudulent conveyance** was configured as a **special crime 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 entity**.

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

The Ruling concluded that both appellants exercised **effective control over the companies involved and orchestrated the sale of assets to avoid the payment of labor 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 for several offenses** of VAT and corporate tax fraud for the years 2011 and 2012.

Specifically, regarding 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**, emphasizing that the same, as a whole, was used to commit the tax offenses. Finally, the Supreme Court clarified that **the penalties imposed** on both the individual and the legal entity, despite the arguments of the defense regarding a possible duplication of the financial burden, were absolutely **proportional to the seriousness of the facts.**

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

The Ruling of the Supreme Court, STS 298/2024, resolves a cassation appeal filed by several of those convicted of crimes against the Spanish Public Treasury and forgery of documents. The case involves mainly three legal entities and their respective owners.

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

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

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

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

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

The **search of the purse** 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 in Spanish).

The lack of observance of these legal guarantees led the High Court of Justice of Andalusia to declare the **dismissal null and void**, since the record, without the proper guarantees, **lacked evidentiary 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 record cannot be used to justify the dismissal. Furthermore, it is emphasized that compliance with these rules is essential to **protect the rights of workers and maintain the integrity of the disciplinary process.**

In this case, the criminal liability of the legal entity is focused on its failure to ensure that the search of the employee's purse 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 the lost wages.**

MOLINS Compliance

Decision of the National Audience Court, Criminal Chamber, of 12 July, 2024.

By means of this decision, the National Audience Court deals with a **case of tax fraud and documentary falsifications** in which multiple legal entities participated.

This decision is of special interest to the extent that the Court considers as a **relevant element for the basis of the criminal liability** of legal entities (specifically, determining it as a negative element of the type) the **absence of adequate control and supervision measures for the fulfillment of their ordinary tax obligations.**

Specifically, it establishes that the **non-payment of the corresponding taxes** is criminally imputable to legal entities due to **the lack of supervision and control measures for the fulfillment of these tax obligations**.

Thus, the **implementation of robust financial controls**, or even the **implementation of a Tax Compliance Management System** based on or inspired by the provisions of the **UNE 19602 standard**, is of utmost relevance. Not only for the purpose of obtaining **a possible exemption from criminal liability**, but also for the **purpose of avoiding the attribution of criminal liability to the legal entity** in the first place.

Decision 559/2024 of the Provincial Court of Mallorca, of 16 December, 2024.

In this ruling, the Provincial Court of Palma de Mallorca convicts a meat products company, as well as one of its administrators, of a **crime against public health** under art. 359 of the Penal Code, due to a serious and general breach of **food safety regulations**.

This Ruling is extremely interesting for its analysis of the **criminal liability of administrators**. In this context, it is worth highlighting the following arguments:

- The ruling indicates that **art. 31 SCC cannot be interpreted as a presumption of guilt of corporate administrators**.
- In this sense, **it is not enough to prove the condition of administrator or legal representative**, but it **must be demonstrated that this natural person has intervened causally, through actions and omissions** in the criminal act.
- As regards the **ways of attributing criminal liability to directors -particularly with respect to the way of omission-**, the concept of the **"duty of diligence**" is essential.
- In order to **define the concept of the duty of diligence**, the Court establishes a relationship between **art. 31, 31 bis SCC and art. 225.2 of the Capital Companies Law (hereinafter, LSC)**. In particular, the Court understands that the **"precise measures"** referred to in art. 225.2 LSC include the **"suitable and effective means"** of article 31 bis SCC, in order to understand a Compliance System as effective.
- However, the Court argues that **the mere implementation of a Compliance System will be insufficient to understand that a director has complied with his duty of diligence** and should not be deserving of a criminal sanction.
- Specifically**, the duty of diligence** of the administrators **will not be fulfilled with the mere incorporation of a Compliance System without any connection or analysis of the business reality and the circumstances in which the activity is carried out.**
- **Thus, it will be essential to adopt a truly customized and implemented Compliance System for the protection of directors and other members of the governing bodies and senior management of legal entities.**

Other agreements and sanctioning resolutions on Compliance

MOLINS
Compliance

- Theft of 23.7 million euros through artificial intelligence fraud.
- 32 million fine to Amazon for going too far in the surveillance of its employees.
- BBVA, sanctioned with 200,000 euros for including a customer in the debt collection file without prior notice.
- The National Audience Court puts on the stand the world's largest exporter of bluefin tuna for resorting to illegal fishing, not respecting health standards and laundering.
- The CNMC investigates the Apple Group for possible anti-competitive practices related to the distribution of apps on its devices.
- Uber fined 290 million for sending data on its drivers to the US despite the prohibition of the CJEU.
- 4.75 million euro fine on Netflix for concealing information on the use of personal data.
- AEPD fines a Spanish company 365,000 euros for making its employees sign in with fingerprints.
- Santander, BBVA and Telefónica dismiss 590 workers due to complaints from colleagues.
- Adidas executives in China investigated in a case of alleged corruption.

Other agreements and sanctioning resolutions on Compliance

MOLINS Compliance

23.7 million euros stolen through an artificial intelligence fraud

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

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 (6) arrests related to the case, highlighting concerns about the increase in this type of fraud with the advancement of generative artificial intelligence technologies.

32 million fine for Amazon for going too far in employee surveillance

The **French Data Protection Agency** (CNIL) **has fined** Amazon *France Logistique* **€32 million for a labor monitoring system** deemed "excessively intrusive."

This system, which involves scanners to measure in real time the productivity of employees has been criticized for **violating the right to privacy and the principles of the French Labor 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 labor efficiency, announcing its intention to appeal the decision.

BBVA fined 200,000 euros for including a customer in the debtors' 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 the file of defaulters without prior notice.

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

These facts constitute an **infringement of article 5.1.d) of the General Data Protection Regulation**, which requires the accuracy of the personal data collected, updating them when necessary.

The National Audience Court puts on the stand the world's largest exporter of bluefin tuna for resorting to illegal fishing, not respecting sanitary regulations and money laundering.

The National Audience Court has agreed to judge eight (8) individuals and twelve (12) entities linked to the largest bluefin tuna exporting group in the world for **alleged commercialization of this species obtained through illegal fishing**. According to the order, the activity was carried **out without the required legal authorizations**, in violation of national and international regulations, and **using facilities that did not comply with the minimum sanitary conditions**, which posed a **risk to public health**.

The order for the transfer to abbreviated proceedings also **indicates** that the profits derived from this activity were subject to **money laundering** through **corporate structures specifically designed to conceal their illicit origin**. This case, which combines crimes against natural resources, public health and money laundering operations, emphasizes the importance of **regulatory compliance in regulated sectors** such as fishing and food, as well as the possibility that any corporation, despite not being considered a regulated entity, can be the active subject of a money laundering crime.

Other agreements and sanctioning resolutions on Compliance

The CNMC investigates the Apple Group for possible anticompetitive practices related to the distribution of applications on its devices

The CNMC is investigating Apple **for possible anticompetitive practices in the distribution of applications through its App Store**. It is suspected that the company could be imposing on developers the **mandatory use of certain payment systems** and restricting other commercial options, which could constitute an abuse **of dominant position**, prohibited by the Antitrust Law and the TFEU.

The investigation was initiated ex officio due to the growing importance of app stores in the digital economy. If the practices are confirmed, they could qualify as a very serious infringement of competition law.

New reform of the Corporate Spanish Criminal Code in sight. Directive 2024/1226 of April 24: new offenses and sanctions for "disobedience"

European Union Directive 2024/1226 establishes that **non-compliance with EU restrictive measures shall be criminally sanctioned**. The criminalized conducts include the **misuse of funds or economic resources subject to restrictions**, the **carrying out of prohibited activities** such as imports, **exports or transfers of restricted goods** and services, and the **facilitation of access or transit of natural people** in contravention of these measures.

To be considered criminal, these actions **must be carried out intentionally**, although in cases involving **goods and services** they may also be punishable for **gross negligence**, unless the value affected is less than 10,000 euros, according to national criteria.

The Directive **extends criminal liability to legal people** when these offenses are committed within and for their benefit. It also **introduces sanctions** such as the **publication of sentences**, which will require Spain to adapt its Spanish Criminal Code to include these provisions, reinforcing Compliance obligations in relation to EU regulations and consequently **imposing due diligence obligations on legal people as prevention and control measures.**

Netflix fined €4.75 million for withholding information on use of personal data

The **Dutch Data Protection Authority** has fined the streaming platform for **failing to comply with the transparency obligations** set out in the RGPD between 2018 and 2020.

In this regard, Netflix **failed to adequately detail** how it treated its **users' personal data**, violating their information rights. Despite subsequent updates to its privacy policy, the body considered that the seriousness of the irregularities justified the financial penalty.

Other agreements and sanctioning resolutions on Compliance

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

The **Spanish Data Protection Agency has fined a Spanish company €365,000** for **requiring 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 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 employees for complaints from colleagues

During 2023, **Santander, BBVA and Telefónica dismissed a total of 590 employees due to complaints from colleagues** filed through internal whistleblower channels.

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

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

Adidas executives in China investigated in alleged corruption case

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

Specifically, this accusation is based on several **screenshots** in which it is alleged that the executives **received bribes and other physical gifts**, such as real estate, from external **service providers in order to obtain the formalization of the contract between Adidas and them.**

Guides, institutional resolutions and reports of interest

MOLINS Compliance

- ISO 42001, Artificial Intelligence Management Systems.
- ISO 45004, Occupational Health and Safety. Occupational Health and Safety Management Systems. Performance evaluation.
- UNE 15713, Secure destruction of confidential and sensitive material.
- UNE-ISO 53800, Guidelines for the promotion and implementation of gender equality and women's empowerment.
- UNE-ISO 37008/TS, Internal investigations of organizations. Guidance.
- CNMC's “Guide for the quantification of damages for infringements of competition law”.
- 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.
- Publication of the resolution to the most frequently asked questions on Law 2/2023, of February 20, regulating the protection of people who report regulatory violations and the fight against corruption by the Anti-Fraud Office of Catalonia.
- Update on the U.S. Department of Justice Guide for the Evaluation of Compliance Systems.

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, the ISO and IEC organizations have developed ISO/IEC 42001:2023 standard.

This initiative responds to the need to properly **manage** the **risks** and **maximize 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 organizations to identify and mitigate risks, ensuring legal compliance and data protection. It also prioritizes human well-being and safety in the **design and deployment of AI systems**, thus contributing to **business resilience and sustainability.**

ISO 45004, Occupational Health and Safety. Occupational Health and Safety Management Systems. Performance assessment

ISO 45004:2024 standard provides guidance for organizations of any type to have **indications on how to proceed in the following aspects**:

- Establishment of **processes for monitoring, measuring, analyzing and evaluating occupational health and safety** (SST in Spanish) performance.
- **Developing relevant indicators** to measure the success of their SST initiatives.
- **Determining Compliance with SST outcomes** and objectives.
- Identification of **areas for improvement and implementation of measures** to improve organizational efficiency and productivity.

The implementation of ISO 45004:2024 enables companies to **improve SST performance and demonstrate the effectiveness of their management systems**, provide greater **confidence to stakeholders**, proactively **identify and address** SST risks, 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 safely carrying out the physical destruction **processes of confidential and sensitive material within 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, is the **registration of the process**, from collection to **destruction, outsourcing, confidentiality agreements staff, collection and transport of confidential and sensitive material,** as well as the **storage and preservation** of such material in the destruction facility.

Guides, institutional resolutions and reports of interest

MOLINS Compliance

UNE-ISO 37008/TS, Internal investigations of organizations. Orientation

The **UNE-ISO/TS 37008:2024** standard responds to the need for rigorous and effective management of internal investigations within organizations. It includes from the **definition of fundamental principles and processes** to the establishment of clear **policies and procedures** for the **execution of investigations**, the communication of their results and the adoption of corrective measures when necessary.

The CNMC's "Guide to the Quantification of Damages for 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),** establishes 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 dominant position.

In its new guidelines, the CNMC emphasizes the importance of **adopting robust and consistent approaches in the quantification of damages**, including methods such as comparative analysis, econometric models and the evaluation of financial and commercial data. It also stresses the need to adequately consider the economic and sectoral context in which the 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

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, evaluates the possibility of **processing personal data** received through the Internal Information System (SII) for **purposes other than those established by Law 2/2023**, which protects whistleblowers from regulatory breaches.

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

In this opinion, 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, allowing further processing when these are compatible** with the **reasonable expectations** of data subjects and always ensuring **adequate protection of personal data** as established by current regulations and data protection principles.

Resolution of the most frequently asked questions on Law 2/2023, of 20 February, regulating the protection of people who report on regulatory infringements and the fight against corruption 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 people who report regulatory infringements and the fight against corruption.

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

- What are the obligations arising from the entry into force of Law 2/2023?
- Do people who report an infringement falling within the scope of Law 2/2023, through the internal channel of a non-obligated entity, enjoy protection from 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 regard, it is important to note that the Anti-Fraud Office of Catalonia **has updated the form** for notifying the appointment and dismissal of the individual or individuals who are part of the collegiate body designated as responsible for the internal information system. This form is **available on its web page**.

Update to the U.S. Department of Justice's Guidance for Compliance Systems Assessment

The **U.S. Department of Justice** updated in September 2024 its **guidance for the assessment of Compliance Systems**, with an emphasis on their effective design, genuine implementation and ability to prevent and detect wrongdoing. The update highlights the **risks associated with artificial intelligence**, urging organizations to **implement ethical controls, active monitoring and policies** to ensure its use complies with the law.

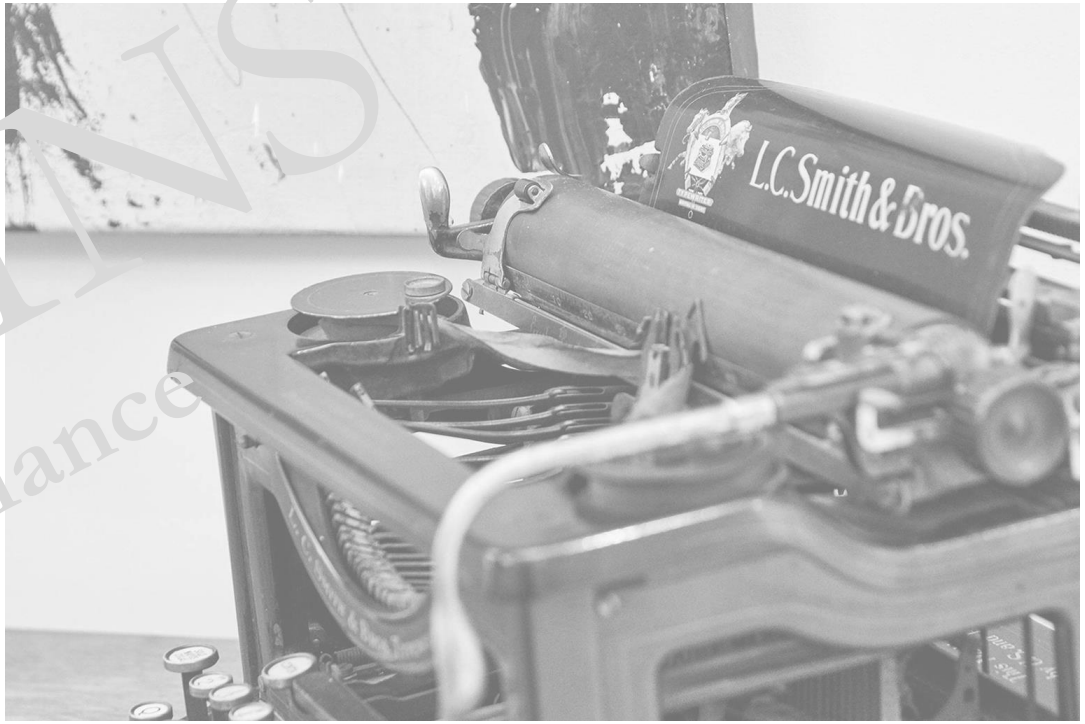
In addition, it reinforces the importance **of ethical channels and anti-retaliation policies**, requiring **training** and **awareness for employees** on internal and external reporting channels. It also addresses the integration of compliance **in mergers and acquisitions processes**, both upstream and in subsequent audits, ensuring the **alignment of the acquired** entity with existing controls.

In short, the guide reminds us that a Compliance System must be **dynamic and capable of evolving** in the face of **new risks**, highlighting **continuous training** based on lessons learned.

Compliance Department publications (January-December 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.
- On 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 1769/2023, of 11 December 2023, of the Second Chamber of the Constitutional Court.
- The challenges 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.



Compliance Department publications (January-December 2024)

MOLINS
Compliance

- Spain continues its fight against corruption: A detailed analysis of judicial developments in 2023.
- Three notes on criminal liability of legal people: Judgment No. 298/2024 of 8 April, 2024.
- Progress in the implementation of the Independent Whistleblower Protection.
- 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?
- Certification according to the UNE 19601 standard: a strategic move to achieve excellence in Compliance.
- Update of the U.S. Department of Justice Guidance on the Evaluation of Corporate Compliance Programs.
- Corporate sustainability moves forward: green light for the proposed Law of Corporate Reporting on Sustainability.

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