MOLINS

Defensa Penal **Compliance**

Compliance Newsletter Year Review

2025

Index

Introduction

MOLINS Compliance

Compliance has positioned itself as a key element in ensuring the soundness and ethics of organisations in today's complex and dynamic regulatory environment. In this context, **continuous updating is not only a duty** but also an **indispensable strategic necessity** for addressing present and future challenges.

During 2025, there have been **significant regulatory and jurisprudential developments in the area of Compliance**, both nationally and internationally. Specifically, there have been developments such as:

- The **Draft Organic Law that will amend the Organic Law on the Criminal Code** for the transposition of Directive (EU) 2024/1226 on offences and penalties for the violation of restrictive measures of the Union.
- The **Supreme Court's new criterion** regarding the **burden of proof** for both the **commission of the offence by the individual** and the **existence of organisational non-compliance** by **the company** (Supreme Court Ruling 768/2025 of 25th September).

In this context, the Compliance Department of **Molins Defensa Penal** has prepared this Newsletter as a review of the main milestones in Compliance for the year 2025. Its content is structured as follows:

- An analysis of the most **relevant legislative developments** that impact the configuration and improvement of compliance systems will be carried out.
- Afterwards, there are some noteworthy **court rulings on Compliance matters** handed down in 2025.
- Next, other significant **agreements and disciplinary resolutions** in the field of Compliance will be presented.
- A brief presentation of **guidelines, institutional resolutions and recent reports** of particular interest will also be included.
- Finally, this Newsletter will conclude with a summary of the **Compliance Department's publications** for the year 2025.

New legislation

MOLINS
Compliance

- Draft Organic Law for the transposition of 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 Directive 2).
- News about Regulation (EU) 2024/1689 on Artificial Intelligence.
- Draft Law 121/46 of 4 February 2025 on transparency and integrity in the activities of interest groups.
- Temporary suspension of the United States (Foreign Corrupt Practices Act).
- New Guidelines from the US Department of Justice (DOJ) on FCPA Investigations and Enforcement.
- Royal Decree 102/2025, of 18 February, amending the Statute of the Independent Whistleblower Protection Authority, A.A.I., approved by Royal Decree 1101/2024, of 29 October.
- Royal Decree 328/2025, of 15 April, appointing Mr Manuel Villoria Mendieta as President of the Independent Authority for the Protection of Whistleblowers (A.A.I.).
- Directive (EU) 2025/794 of the European Parliament and of the Council of 14 April 2025 amending Directives (EU) 2022/2464 and (EU) 2024/1760 as regards the dates from which Member States are to apply certain requirements for sustainability reporting and due diligence by companies.
- European Parliament legislative resolution on certain corporate reporting and due diligence requirements for companies in relation to sustainability.
- Draft Law for the proper use and governance of Artificial Intelligence, adapting to Regulation (EU) 2024/1689 on Artificial Intelligence.
- Order PJC/908/2025, of 8 August, determining the date of commencement of operations of the Independent Whistleblower Protection Authority, A.A.I.
- Commission Delegated Regulation (EU) 2025/2003 of 8 September 2025 amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items.
- Royal Decree-Law 10/2025, of 23 September, adopting urgent measures against genocide in Gaza and in support of the Palestinian people.
- Draft Organic Law amending Organic Law 10/1995 of 23 November on the Criminal Code, transposing Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and sanctions for the violation of Union restrictive measures, and amending Directive (EU) 2018/1673.

New legislation

Draft Organic Law for the transposition of 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 Directive 2)

On 14 January 2025, the Council of Ministers approved the Draft Law on Cybersecurity Coordination and Governance, with the aim of **transposing Directive (EU) 2022/2555 (NIS-2)**, in force since January 2023. This Directive encompasses a set of **measures aimed at ensuring a high common level of cybersecurity throughout the EU**.

The Draft Law extends the scope of the NIS-2 Directive to include, in addition to the sectors already covered (energy, transport, banking, healthcare, water, public administration, digital infrastructure and technological services), the nuclear industry as a high-risk sector. It also incorporates the private security sector into the group of medium-criticality sectors, along with waste management, food production and distribution, postal services and scientific research.

It also specifies the **scope of application** in public or private entities that are tax residents in Spain or that, while resident in another EU Member State, offer their services or carry out their activities in Spain. These entities must carry out an individualised risk assessment and establish measures to guarantee and raise the security levels of their networks and information systems, as well as prevent the risk of incidents.

The text provides for the creation of the **National Cybersecurity Centre**, which will act as the coordinating body at national level and point of contact with the EU, and will be responsible for drawing up the list of entities considered essential or important.

In addition, the draft bill establishes the obligation to **appoint an information security officer**, who will be responsible for developing cybersecurity strategies and policies, supervising their implementation, managing incidents, ensuring compliance with the security criteria established by external providers, and acting as a point of contact with the supervisory authorities. Furthermore, in essential entities, this officer must be accredited by the Ministry of the Interior.

News about Regulation (EU) 2024/1689 on Artificial Intelligence

Although the Regulation was not approved in 2025, it should be noted that **some of its provisions have come into force this year**, taking into account the progressive implementation provided for in the Regulation itself until August 2026. Specifically, the following provisions have been applicable since **2 February 2025**:

- Chapter I on **general provisions**, including the **definition of Artificial Intelligence** (hereinafter, AI) **systems** and **AI literacy**. It stipulates that suppliers and those responsible for implementing AI systems must take measures to ensure that, as far as possible, the people who operate or use such systems have adequate training in the field.
- Chapter II on **prohibited practices**. Some of the most notable are as follows:
    - The use of AI systems that employ subliminal or manipulative techniques that substantially alter people's behaviour and informed decision-making capacity.
    - The use of AI systems that exploit vulnerabilities (age, disability or socio-economic status) in order to substantially alter their behaviour.
    - Classifying individuals based on their behaviour or characteristics if this leads to unjustified, disproportionate or out-of-context treatment.
    - Classifying individuals using biometric data in order to infer sensitive aspects such as race, ideology or sex life, except in legal contexts or for lawful data processing.

To clarify some of the above provisions, the **European Commission has published guidelines** on the subject to address certain undefined legal concepts.

Furthermore, in line with the Regulation's phased implementation schedule, the provisions relating to obligations for AI model providers and certain aspects of penalties to be provided for by Member States will also take effect on **2nd August 2025**.

New legislation

MOLINS Compliance

Draft Law on transparency and integrity in the activities of interest groups

On 4th February, the Government promoted the Draft Law on Transparency and Integrity in the Activities of Interest Groups, with the **aim of regulating, within the scope of the General State Administration and the institutional public sector, the relations between interest groups** (also known as lobbies) and public officials, in accordance with **criteria of transparency, integrity and equality**.

The following new features stand out:

- Creation of the **Register of Interest Groups**, which is mandatory, public, free and electronic, managed by the Conflicts of Interest Office.
- **General prohibition** of contact with public officials **without prior registration** in the Register.
- The concept of the '**regulatory footprint report**' is introduced, which must be included in regulatory files to reflect which lobbyists have participated in the drafting of each regulation.
- **Binding code of conduct** for interest groups.

It should be noted that, in September 2025, **amendments to the articles presented by the Government** were published by the various parliamentary groups during the processing of the Bill in Congress.

Temporary suspension of the United States Foreign Corrupt Practices Act (FCPA) and new enforcement guidelines

On 10 February 2025, United States (hereinafter, US) President Donald J. Trump signed Executive Order (hereinafter, EO) entitled '**Pausing FCPA Enforcement to Promote US Economic and National Security**', instructing the Department of Justice (hereinafter, DOJ) to **suspend the initiation of new investigations** or proceedings under the FCPA for an initial period of **180 days**, with the possibility of extending for another 180 days if the Attorney General deemed it appropriate.

During this hiatus, the EO primarily requires:

- A **comprehensive review of** FCPA enforcement **guidelines** and policies, both for ongoing and past cases, in order to '**restore appropriate boundaries**'.
- The **issuance of new guidelines**, aligned with the country's foreign policy, the economic competitiveness of the United States, and the rational use of federal resources (*see the following section on the new guidelines issued in this area*).
- **Suspension of new investigations**, except with the express authorisation of the Attorney General in cases of 'individual exception'.

New Guidelines from the US DOJ on FCPA Investigations and Enforcement

On 9th June 2025, the US Department of Justice issued a new memorandum with the **aim of aligning the application of the FCPA with the guidelines set out** in the OE of 10th February, signed by President Trump. The document **expressly reaffirms the need for exceptional prior authorisation to initiate any new investigation**.

It establishes a **more selective framework for the application of the FCPA**, aimed at:

- Limit undue burdens on US companies operating abroad.
- Focus sanctions on conduct that directly compromises 'national interests'.

Prosecutors should **prioritise the investigation of cases with strong evidence of criminal conduct attributable to individuals**, avoiding generic charges against corporate structures, and weighing the potential collateral effects on employees.

In addition, **any new FCPA investigation must be authorised in advance by the Assistant Attorney General** or a higher authority. Key **factors** that will guide the decision to initiate or continue investigations include:

- The **fight against cartels and transnational criminal organisations**, especially when bribery facilitates their operations, money laundering mechanisms are used, or they are linked to public officials.
- The **protection of free competition**, in cases of economic damage to US entities.
- The **safeguarding of national security**, in strategic sectors.

New legislation

- The seriousness of the conduct, **excluding routine business practices or permitted courtesies**, and focusing the investigation on significant payments, as well as sophisticated concealment and fraud schemes.

Finally, it should be noted that these guidelines are not exhaustive and that **all current and future research must comply with these new criteria**.

Royal Decree 102/2025 and Royal Decree 328/2025

In order to comply with **Law 2/2023**, the Statute of the Independent Whistleblower Protection Authority (hereinafter referred to by its Spanish acronym, A.I.P.I.) was established in 2024. The A.I.P.I. is an independent **administrative authority at the state level** and has its own legal personality. Among its aims, the A.I.P.I. **seeks to guarantee the protection of whistleblowers** and serve as an **essential institutional pillar in the fight against corruption, acting** in **coordination**, where appropriate, with **other administrative bodies or supervisory, control, inspection or investigation bodies** with similar functions already existing at the national and regional levels, as well as with authorities with similar functions in their respective areas.

On 18 February, **Royal Decree 102/2025** amended various aspects of the Statute. Specifically, a new section was added to Article 1, stating that the A.I.P.I. will have its headquarters in the city of Madrid, granting it new functions and allowing it to request technical reports from both the public bodies affected by the circulars and the internal bodies of the A.I.P.I.

Finally, by **Royal Decree 328/2025**, on 15th April 2025, **Mr. Manuel Villoria Mendieta** was appointed President of the A.I.P.I.

Directive (EU) 2025/794 of the European Parliament and of the Council of 14 April 2025 amending Directives (EU) 2022/2464 and (EU) 2024/1760 as regards the dates from which Member States are to apply certain requirements for sustainability reporting and due diligence by companies

On 14th April 2025, **Directive (EU) 2025/794**, known as '***Stop the Clock***' or the **Temporary Suspension Directive**, was approved. This regulation introduces a postponement in the entry into force of various corporate reporting and sustainability due diligence requirements, with the aim of giving companies more time to adapt to these obligations without incurring disproportionate costs.

The Directive is part of the so-called Omnibus Package, an initiative of the European Commission aimed at simplifying and reducing administrative burdens for companies in the area of sustainability, especially small and medium-sized enterprises.

Among the main measures included in the Directive is a **two (2) year** deferral in the application of the reporting requirements set out in the **Corporate Sustainability Reporting Directive (hereinafter CSRD)** for certain companies:

- From **1st January 2027**, large companies that are not yet subject to the Non-Financial Reporting Directive will be required to submit their sustainability reports for the 2028 financial year.
- From **1st January 2028**, listed SMEs, captive insurers considered large, and small and non-complex credit institutions must submit their reports for the 2029 financial year.

Likewise, the regulation **postpones** the entry into force of the **Corporate Sustainability Due Diligence Directive (hereinafter, CSDDD)** by **one (1) year.**

European Parliament legislative resolution on certain reporting requirements

On 16 December 2025, the European Parliament plenary session approved an important **provisional agreement** that could affect several of the **directives** that make up the **Omnibus I package**, specifically the CSRD Directive and the CSDDD Directive. However, this text must be formally validated by the Council in January 2026.

From a corporate compliance perspective, the changes introduced by this revision are significant and operate in two (2) main areas:

- **Corporate Sustainability Reporting Directive** (CSRD): The **threshold for compliance is raised significantly**, so that only companies with **more than 1,000 employees and a net turnover of more than €450 million** will be required to report under the CSRD from 1st January 2027, drastically reducing the number of entities subject to the directive.

New legislation

Furthermore, **the information that can be requested in the value chain is limited**, introducing criteria of proportionality and reasonableness and reducing indirect burdens on smaller suppliers.

- **Corporate Sustainability Due Diligence Directive** (CSDDD): As in the case of the previous Directive, the thresholds for the application of this Directive are substantially increased, **significantly reducing the number of companies subject to due diligence obligations**. It should be noted that the transposition and entry into force of these obligations will be postponed for most companies until July 2029, offering a longer transition period for their implementation.

This revision reflects **an approach of regulatory simplification** that seeks to **balance the requirement for transparency and due diligence** with a **reduction in the subjective scope of its application, more flexible reporting obligations and longer adaptation periods**, which will have a significant impact on the corporate Compliance strategies of European companies and those operating in the EU.

In Spain, regulatory uncertainty regarding sustainability is more pronounced than in other Member States. In addition to the revision of EU regulations, there are the effects of the delay in transposing the **CSRD and the *Stop the Clock* Directive**, which further complicates the business landscape.

Draft Law for the proper use and governance of Artificial Intelligence

On 11th March 2025, the Council of Ministers approved the **Draft Bill for the proper use and governance of AI,** in response to **Regulation (EU) 2024/1689**. Despite the direct applicability of the Regulation, many of its provisions require national legislative development for their correct implementation.

In this context, issues such as the following are specifically regulated:

- Those **responsible for supervising and sanctioning** AI systems depending on the sector. For example, the Spanish Data Protection Agency for security systems or the General Council of the Judiciary for justice administration systems.
- The **designation as the notifying authority** of the Secretary of State for Digitalisation and Artificial Intelligence.
- The appointment of the Spanish Agency for the Supervision of Artificial Intelligence as the **competent national authority responsible for establishing a controlled testing space for AI**.

Order PJC/908/2025, of 8th August, determining the date of commencement of operations of the Independent Whistleblower Protection Authority

As mentioned above, **Law 2/2023** of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, **authorised in Title VIII the creation of the A.I.P.I.**

To this end, Royal Decree 1101/2024, of 29 October, **approved the Statute of the A.I.P.I.** The Transitional Provision of the aforementioned Royal Decree establishes a period of **two months to communicate the appointment of the Head of the Internal Information System**. To this end, it is hereby announced that the A.I.P.I. will begin to count this period from the moment the specific notification form for the head of the internal channel is published on its official website (which, as of the date of this Newsletter, has not yet been published).

It should be noted that all obligated parties must send the A.I.P.I. the notification of the Head of the Internal Information System, regardless of whether it is also sent to any regional authorities that may exist.

The aforementioned Order established **1 September 2025** as the date on which the A.I.P.I. will become operational. Likewise, in order to guarantee its operability in the initial phase, it was agreed that, **until 1st November 2025**, the Ministry will continue to provide certain support services so that it can carry out its activities during this period with **full respect for its functional autonomy and independence**.

Commission Delegated Regulation (EU) 2025/2003 of 8 September 2025 amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items

The Delegated Regulation of 8th September 2025 marks a **significant milestone** in the evolution of European policy on the control of dual-use goods.

Dual-use goods comprise those **products**, including software and technology, that can have both **civil** and **military** or **nuclear applications**.

New legislation

The Control List, which is usually updated **annually**, incorporates a **new regulatory block** in this revision that focuses specifically on **quantum and cryogenic technologies**, recognising their growing importance.

In addition, equipment and materials for the manufacture and testing of **semiconductors, advanced integrated circuits and electronic assemblies, coatings** for high-temperature applications, **additive manufacturing machines** (3D printing), among others, have been included within dual-use goods.

From a compliance perspective, this update reinforces the need for organisations to effectively **integrate export controls** into their **compliance systems**, incorporating mechanisms for identifying, assessing and managing **regulatory risks associated** with the **international trade of dual-use goods**, in line with a prevention and enhanced due diligence approach.

Royal Decree-Law 10/2025, of 23rd September, adopting urgent measures against genocide in Gaza and in support of the Palestinian people

Royal Decree-Law 10/2025, of 23rd September, **came into force on 24th September 2025** and was ratified by the Congress of Deputies on 8th October 2025. This Royal Decree-Law regulates four (4) fundamental aspects:

- **Article 1. Prohibition on transfers of defence and dual-use material:** This article establishes a prohibition on exporting to Israel and importing from Israel defence material and dual-use products, in accordance with the annexes to Royal Decree 679/2014 of 1st August. Some of the products included therein are:

(i) chemical compounds; (ii) reactors, tanks and mixing equipment designed to handle hazardous chemicals; (iii) equipment and valves for containing corrosive or toxic gases; (iv) industrial or military precision flow and pressure control equipment; (v) reactive materials produced by selective laser synthesis. Likewise, there is an obligation to deny requests for authorisation to transit the aforementioned material.

- **Article 2. Fuels for military use destined for Israel**: The Royal Decree-Law extends the ban to the transit of fuels susceptible to military use to Israel. Therefore, the previous exception applicable to JP-4, JP-5 and JP-8 aviation fuels is removed, so that their transit will also be denied. Likewise, any other fuel with potential military end use, if destined for Israel, will also be automatically denied.
- **Article 3. Prohibition on customs imports of products originating in Israeli settlements:** The Royal Decree-Law prohibits the import of products originating in Israeli settlements in the Occupied Palestinian Territory. From 25th September 2025, all customs declarations for goods originating in Israel must include detailed information on their place of origin, including the postcode and town of origin. The State Tax Administration Agency will have the power to refuse the importation of products from these settlements, and non-compliance will be punished in accordance with Organic Law 12/1995 on the Suppression of Smuggling, with prison sentences and fines.
- **Article 4. Illegal advertising**: The Royal Decree-Law considers the advertising of products and services originating in settlements in the Occupied Palestinian Territory to be illegal.

Draft Organic Law amending Organic Law 10/1995 of 23rd November on the Criminal Code, transposing Directive (EU) 2024/1226 of the European Parliament and of the Council of 24th April 2024 on the definition of criminal offences and sanctions for the violation of Union restrictive measures, and amending Directive (EU) 2018/1673

On 25th March 2025, the Government approved the **Draft Organic Law amending the Criminal Code**, with the aim of transposing **Directive (EU) 2024/1226**, which establishes minimum standards for classifying **serious infringements of restrictive measures imposed by the EU as criminal offences, for which legal persons may be held criminally liable**.

New legislation

The main **new features of the Draft Law** are as follows:

- **Increase the penalty for the upper half of the crime of receiving stolen goods and money laundering** when the goods originate from non-compliance with EU restrictive measures.
- Creation of a new title: **Title XXIII *bis* in Book II of the Criminal Code entitled 'Offences against the area of freedom, security and justice of the European Union',** which ensures that the conduct defined therein constitutes an offence when it is intentional and violates a prohibition or obligation that constitutes an EU restrictive measure.
- **Offence of violation of EU restrictive measures**: punishes illegal operations when the value of the goods or services exceeds EUR 10,000, or whenever they involve military equipment or dual-use products.
- **Offence of circumvention of restrictive measures**: punishes failure to comply with the obligation to report funds or economic resources subject to restrictions.
- **Offence of facilitating entry or transit**: penalises allowing sanctioned natural persons to enter or transit through EU territory.

Likewise, on **31st October 2025**, the **Draft Organic Law for the transposition of Directive 2024/1226 on the definition of offences and penalties for the violation of Union restrictive measures was officially published in the Official Gazette of the Spanish Parliament**. The main objective is to harmonise Spanish legislation with European regulations, strengthening the effectiveness of the penalties imposed by the EU.

At the time of publication of this Newsletter, the Draft Law is in the process of being amended by the Justice Committee.

Case law

- Decision of the National Audience Court, Criminal Chamber, Appeals Section, 4/2025, of 21 January 2025, Rec. 23/2024.
- Decision of the Supreme Court, Second Courtroom of the Criminal Chamber, 223/2025, of 12 March 2025, Rec. 5765/2025.
- Decision of the Supreme Court, Second Courtroom of the Criminal Chamber, 372/2025, of 11 April 2025, Rec. 7151/2022.
- Decision of the Supreme Court, Second Courtroom of the Criminal Chamber, 379/2025, of 30 April 2025, Rec.
- Decision of the High Court of Justice of Catalonia, Contentious-Administrative Chamber, Section 5, 1572/2025, of 5 May 2025, Rec. 809/2023.
- Decision of the Supreme Court, Third Courtroom of the Contentious-Administrative Chamber, Section 4, 704/2025, of 4 June 2025, Rec. 2188/2023.
- Decision of the High Court of Justice of Madrid, Labour Chamber, 441/2024, of 5 June 2025, Rec. 441/2025.
- Order of the Provincial Court of Oviedo, Section 2, 410/2025, of 18 June 2025, Rec.
- Decision of the National Audience Court, Criminal Chamber, 9/2025, of 2 July 2025.
- Decision of the General Court of the European Union, Tenth Chamber, of 3 September 2025. T-533/2023 (Latombe v Commission).
- Decision of the Supreme Court, Second Criminal Chamber, Decision 768/2025, of 25 September, Rec. 1008/2023.
- Decision of the Supreme Court, Second Criminal Chamber, Decision 836/2025, of 14 October, Rec. 432/2023.
- Order of the National Audience Court, Criminal Chamber, Section 2, 753/2025, of 10 December 2025, Rec. 598/2025.

Decision of the National Audience Court, Criminal Chamber, Appeals Section, 4/2025, of 21 January 2025, Rec. 23/2024

This decision addresses the possible application of the **mitigating circumstance provided for in art. 31 *quater* d) of the Spanish Criminal Code** in a case where a company was convicted of tax fraud, using a **carousel fraud** structure and involving intra-Community commercial transactions.

In its appeal, the company requested the application of this mitigating circumstance, arguing that, **after the commission of the criminal acts and before the start of the trial, it had implemented a Compliance Management System and appointed a Compliance Officer**.

The National Audience Court **rejected the application of the mitigating circumstance, considering that there was no evidence of a real and effective willingness on the part of the company to cooperate and repair the damage**. The court's reasoning is based on the fact that art. 31 *quater* of the Criminal Code requires that such actions demonstrate a clear and effective commitment to the prevention of potential applicable offences. The Court perceived the **measures adopted by the company as formal or superficial (Paper Compliance)** with the sole objective of obtaining the mitigating circumstance and without demonstrating the intention to implement a culture of real compliance.

Decision of the Supreme Court, Second Courtroom of the Criminal Chamber, 223/2025, of 12 March 2025, Rec. 5765/2025

This ruling confirms the **conviction for the crime of asset stripping of two administrators** (one *de facto* and the other *de jure*) and declares the **subsidiary civil liability of the legal entity pursuant to Article 120.4 of the Criminal Code**. The case clearly illustrates how the existence of a corporate structure, without the need for the legal entity to be found criminally liable, **does not exempt the company from civil liability for damages caused by its representatives**.

The company was used as a vehicle to carry out real estate transactions that generated significant VAT revenue (more than €700,000). These amounts were embezzled, causing direct damage to both the Treasury and other creditors. **The company, despite not having been criminally convicted, was declared subsidiarily liable for the acts committed within it**.

The Supreme Court did not assess whether the company had a compliance system with internal controls, noting that **the attribution of civil liability under art. 120.4 of the Criminal Code operates objectively when the offence is committed in the exercise of corporate functions or activities**. Thus, **the implementation of Compliance Systems is not invocable for the exemption from paying compensation**, especially when administrators use the corporate structure to commit crimes.

This reinforces the importance of integrating cross-cutting crime prevention tools such as unfair management, punishable insolvency, and other economic fraud into compliance systems.

Decision of the Supreme Court, Second Courtroom of the Criminal Chamber, 372/2025, of 11th April 2025, Rec. 7151/2022

In this ruling, the Supreme Court **upheld the appeal** lodged by the legal entity convicted in previous instances for aggravated fraud.

The Court thus made it clear that **proving a structural defect in compliance management systems is an essential and indispensable element in attributing criminal liability to legal entities.**

It is worth noting how the Court openly criticises the previous ruling, observing how criminal liability was attributed to the legal entity without individualised grounds, derived solely from the actions of the administrator himself, and ignoring the need to prove a structural defect in the Compliance Management System.

Initially, the organisation was found guilty of fraud consisting of deception in the sale of franchises by its administrator, who was also sentenced to four years in prison. Automatically, and without providing any evidence, criminal liability was attributed to the company for the acts carried out by its administrator.

The Supreme Court reminds judges and courts that **the regime of vicarious liability should not be applied when attributing criminal liability**, since **guilt can only be proclaimed for one's own actions**. In this case, it should have been for the company's lack of prevention or compliance plans to prevent the risk of managers acting outside the law and thus committing fraud.

The ruling also highlights **the importance of legal persons having their own separate defence through which they can assert the principle of contradiction and differentiate the interests of the natural person (administrator) from those of the legal person**.

This ruling provides additional legal certainty for organisations, as it raises the standard of proof required to attribute criminal liability.

Decision of the Supreme Court, Second Courtroom of the Criminal Chamber, 379/2025 of 30th April 2025, Rec. 4603/2022

This Supreme Court ruling addresses a case of serious injuries sustained during an amateur football match, but what is relevant from a compliance perspective are the implications drawn by the SC regarding the **position of guarantor of organisations that promote activities that may involve some risk**.

Although the procedural debate focuses on the violation of guarantees during the trial, what is relevant in terms of compliance is the **Supreme Court's call to strengthen the organisational diligence of entities promoting events**, such as, in this case, non-professional football matches. It thus indicates that these associations, which are legal entities, must **implement effective preventive mechanisms to minimise the risk of criminal conduct by their members or participants, even in the case of informal, sporting or recreational activities**.

This ruling **extends the requirement to prevent criminal conduct** to non-profit organisations or sports associations, which may also face legal consequences if they fail to take reasonable measures to control their activities. This ruling reinforces the need **to extend the practical application of Compliance Management Systems beyond the traditional corporate environment**, emphasising the importance of associations, organisations and other non-profit legal entities establishing preventive measures against undesirable actions that could lead to the commission of crimes. The absence of adequate controls can open the door to subsidiary civil, reputational and even criminal liability.

Decision of the High Court of Justice of Catalonia, Contentious-Administrative Chamber, Section 5, 1572/2025, of 5 May 2025, Rec. 809/2023

The ruling addresses the **assessment of the adequacy and effectiveness of a compliance programme in the field of competition law** as a determining factor in the possible **review of a prohibition on contracting**. The ruling was handed down in the context of a **contentious-administrative appeal** filed by the plaintiff against the **alleged rejection** of its second request to lift the prohibitions on contracting imposed in 2021, basing its claim on the implementation of a Compliance Programme.

The Court starts from an essential premise: **the mere formal existence of a Compliance Programme does not, in itself, prove its effectiveness**. In this context, the High Court of Justice of Catalonia **analyses the material content and practical implementation** of the Programme, identifying a series of **structural deficits** that prevent it from being considered effective.

In particular, with regard **to disciplinary measures**, the Court highlights: (i) the **absence of termination clauses** as a disciplinary measure in the contracts of managers and employees applicable to the entire workforce; (ii) that it is **not sufficient** for staff to be aware of the possible penalty for breaching the Code of Conduct or other Programme documents, given that the introduction of a **termination clause**, especially with regard to employees who participated in the sanctioned conduct, has a **greater deterrent effect**; (iii) the **lack of gradation of offences** and clear identification of offending conduct; and (iv) the **absence of sanctions** for offending staff, which compromises the credibility and preventive capacity of the system.

With regard to **communication and adherence to the Programme**, the following are highlighted: (i) the **lack of effective access** by staff to the model documents and the **absence of a signed commitment**; and (ii) the **absence of compliance commitment clauses**.

In terms of **training and awareness**, the Chamber concludes that there is no evidence of an **effective training plan** and questions the **ineffectiveness of the incentive policy**. With regard to the **reporting channel**, it notes that there is no specification of how to submit **anonymous reports via email**.

Special attention should be paid to the considerations relating to the person responsible for the design and control of the Compliance Programme (**Compliance Committee and Compliance Officer**). The Court notes: (i) a **lack of independence and conflicts of interest**, as the body includes individuals who were involved in the sanctioned conduct; (ii) **insufficient** specialist **knowledge** among its members; and (iii) the **absence of support from external advisers**, a factor which, in contexts of high regulatory complexity, can be decisive in providing technical solvency and credibility to the model.

Finally, in relation to the **risk map**, the Supreme Court identifies substantive shortcomings: (i) not all relevant conduct has been incorporated, including the infringement linked to the second case; and (ii) there is a lack of necessary controls, such as the incorporation of a **clause committing to compliance with competition regulations** in cases of participation in the same tender by companies belonging to the same group.

Decision of the Supreme Court, Third Courtroom of the Contentious-Administrative Chamber, Section 4, 704/2025, of 4th June 2025, Rec. 2188/2023

The ruling is relevant to **internal investigation management procedures** under Law 2/2023. The High Court first recalls that the **principles underlying criminal law are transferable to administrative disciplinary law**.

In this regard, the civil servant was punished for serious disobedience for failing to answer the questions asked by the investigating officer during the preliminary proceedings prior to the opening of disciplinary proceedings, in which civil servants are bound by the principle of cooperation to clarify the facts.

However, the Court emphasises that this right conflicts with another constitutional right, the right not to testify against oneself as a guarantee of the right of defence. Therefore, **the focus must be on each case in order to respect the procedural guarantees involved in these proceedings**. In this case, the facts were clear and the person responsible was identified, coinciding with the civil servant who was part of the preliminary investigation.

In this context, **the Supreme Court ruled in favour of refusing to answer the investigating judge's questions when they were clearly incriminating**. The Court concluded that this **right not to incriminate oneself extends to pre-disciplinary proceedings**, and for this reason, the civil servant could not be sanctioned.

Decision of the High Court of Justice of Madrid, Labour Chamber, 441/2024, of 5 June 2025, Rec. 190/2025

This ruling addresses the disciplinary dismissal of a Managing Director who filed an internal complaint against the HR Director, accusing her of dismissing an employee because of his sexual orientation. What is relevant from a compliance perspective is the High Court of Justice analysis of **the malicious use of the ethics channel, contractual good faith and the limits of whistleblower protection.**

The internal investigation, conducted by the company's Compliance Committee, concluded that **the complaint lacked any evidence and was used to harm a colleague for personal reasons**. The court emphasises that **the purpose of the complaint was not ethical or preventive, but reactive and harmful** to a colleague, turning it into a tool for pressure and personal discredit.

The Supreme Court revokes the lower court's **ruling of unfair dismissal** and classifies it as appropriate, considering that there was a **serious breach of contractual good faith**. It also emphasises that not all internal complaints enjoy automatic protection, **since when a complaint is made without foundation and with harmful intent, this may constitute valid grounds for dismissal**.

This case provides a clear example of how the **protection against reprisals or consequences offered by Law 2/2023 does not cover unfounded or malicious complaints**.

Order of the Provincial Court of Oviedo, Section 2, 410/2025, of 18th June 2025, Rec. 180/2025

The ruling is of particular interest because it includes an explicit analysis of the **whistleblower protection framework provided for in Law 2/2023**.

The case arose from an appeal against the provisional dismissal of proceedings initiated after a complaint was filed, among other facts not covered by the appeal, the existence of an **anonymous email in which the complainant's personal data** (telephone numbers, call lists) was allegedly used and certain behaviours were attributed to him, thus revealing personal information and habits relating to his sex life.

The Chamber focuses its analysis on a key point: the deductions made by the sender of the email — by examining call lists associated with a telephone line and comparing them with contact numbers published on prostitution websites — and the subsequent disclosure of this information to a media outlet, do not constitute unlawful conduct, and in particular cannot be subsumed under the types of **dissemination, disclosure or use of personal data**.

The order adds that the communicator's action falls within the scope of protection defined by Law 2/2023, as it is a communication aimed at revealing a possible irregularity: specifically, the possible unlawful use of a public telephone line assigned to the appellant, completely unrelated to the purposes of his function.

Specifically, **the resolution focuses on the subjective and objective scope of protection, recalling that article 2 of Law 2/2023 protects those who report, through the established procedures, actions or omissions that may constitute a criminal offence or a serious or very serious administrative offence**.

However, the determining factor in the case analysed is the specific reference to article 27, relating to **public disclosure as a means of communication**: it is emphasised that the protection regime under Title VII is applicable without any additional conditions when the person has disclosed information directly to the press in the exercise of freedom of expression and the right to communicate truthful information, in accordance with the constitutional framework and its implementing regulations.

Decision of the National Audience Court, Criminal Chamber, 9/2025, of 2nd July 2025

This July, a company was convicted of subsidy fraud under art. 310 of the Criminal Code in relation to art. 308.1 of the Criminal Code.

In 2018, the company applied for and obtained European public aid from the Spanish Agricultural Guarantee Fund (hereinafter, FEGA) with the aim of carrying out projects for the processing, marketing and development of agricultural products (fruit and vegetables), for a total amount of €3.8 million. At the same time, the company applied for a loan of €6 million from the Catalan Institute of Finance, on which it was granted a 2% interest subsidy by the Directorate-General for Industry.

The conflict arises from the fact that the company did not inform FEGA of the receipt of this subsidy, thereby failing to comply with the obligation to declare other public aid received or requested, which determined the incompatibility between said aid according to the applicable regulations (regional aid corresponding to the interest subsidy and other state aid from FEGA was received).

The company also **requested the mitigating circumstances of art. 31 *quater* c) and d) of the Criminal Code**.

With regard to **compensation for damages** (art. 31 *quater* c) of the Criminal Code), the company merely provided the required financial guarantee, but the judge indicated that **compensation for damages requires payment of the principal amount due and interest,** and therefore**, rejected the application.**

As for the application of the mitigating circumstance under art. 31 *quater* d) of the Criminal Code, the judge accepted it due to the **implementation of certain crime prevention measures prior to the start of the trial**.

Even so, the court expressed certain **doubts about the authenticity of the compliance programme provided** (a due diligence report dated 2017), **as it is a simple, unauthenticated photocopy that was suddenly presented at the trial without any documents having been provided during the investigation phase**, which was not referred to by any of the defendants throughout this phase, and whose existence was not expressly mentioned in the provisional conclusions of the convicted party.

However, **despite its generic content and lack of essential structural elements** (such as control officers or operating protocols), **the court recognises the mitigating value of the compliance programme provided, as it was formally implemented after the events took place**.

Decision of the General Court of the European Union, Tenth Chamber, of 3rd September 2025. T-533/2023 (Latombe v. Commission)

Mr. Philippe Latombe, a French citizen and user of various digital platforms that transfer personal data to the US, brought an **action for annulment** against **European Commission Implementing Decision (EU) 2023/1795**, which approved the **Data Privacy Framework (DPF)** or **Framework for the Transfer of Personal Data between the EU and the US**, arguing that this framework does not guarantee a **level of data protection substantially equivalent** to that required by the General Data Protection Regulation (hereinafter, **GDPR**) and the **Charter of Fundamental Rights**.

The **General Court of the European Union** dismissed the appeal in its entirety and confirmed the validity of the Decision, declaring the level of protection applicable to personal data transferred to the US under the DPF to be **adequate**. Furthermore, for reasons of **good administration of justice**, the Court **refrained from ruling** on the inadmissibility raised by the Commission and went directly to the merits of the case, concluding that the appeal was **unfounded**.

For practical purposes, the Court upheld the standard already established by the Court of Justice of the European Union, reiterating that article 45 of the GDPR requires the third country to ensure a level of protection that is **substantially equivalent, not identical**, and that the Commission's assessment of adequacy is subject **to strict judicial review**.

Decision of the Supreme Court, Second Criminal Chamber, Decision 768/2025, of 25th September, Rec. 1008/2023

The ruling addresses the criminal liability of a **commercial company** accused, together with its administrator, of a **continuing offence of fraud**. The individual had carried out fraudulent activities through false job offers that concealed profit-making training courses. In this regard, **the National Audience Court had considered that the administrator's actions were also attributable to the company, on the understanding that the latter had benefited from the fraud**. However, the **appeal** lodged by the company challenged precisely this automatic extension of liability, arguing that the existence of any organisational defect or ineffective control system that allowed or facilitated the offence had not been proven.

Therefore, in its ruling, the Supreme Court precisely defines the core of the criminal liability of legal persons in accordance with Article 31 *bis* of the Criminal Code, stating that **the attribution of liability to an entity requires proof of a serious organisational defect, i.e. a real lack of control or supervision mechanisms that reveals a breach of the duty to prevent crimes**. It is not enough to prove that a natural person linked to the company committed the crime; it **is also necessary to prove that such behaviour was made possible by a structural failure within the organisation itself**.

The Court also emphasises that **corporate criminal liability cannot be objective or automatic**. It therefore expressly rejects vicarious liability, clarifying that the Spanish model does not allow the guilt of a manager or employee to be transferred directly to **the legal entity and that the entity is only liable when the offence is a manifestation of its own disorganisation or a culture of non-compliance**.

Furthermore, **the burden of proof lies with the Public Prosecutor's Office, which must demonstrate both the commission of the offence by the natural person and the existence of organisational non-compliance on the part of the company**.

Finally, the Supreme Court emphasises that the presumption of innocence also applies to legal persons, and that the lack of evidence of a control defect prevents conviction. In this case, **as it was not proven that the company lacked a reasonable supervision system or that there was an institutional policy of tolerance towards fraud, the Court concludes that there was no organisational fault and therefore acquits the company**.

Decision of the Supreme Court, Second Criminal Chamber, Judgment 836/2025, of 14th October, Rec. 432/2023

In this ruling, **the Supreme Court acquits the legal entity of the crime of concealment of assets because the existence of a structural defect in the company that would have allowed or facilitated the commission of said crime was not proven**.

The Supreme Court emphasises that the **criminal liability of legal entities** does not automatically derive from the criminal conduct of their members, but **requires proof that the offence was committed by a natural person acting in the context of their duties within the company**, in accordance with article 31 *bis* of the Criminal Code. Furthermore, **for a company to be criminally liable, it must also be proven that the organisational structure of the company facilitated or enabled the commission of the offence**.

In this case, the Court emphasises that **it was not proven that the company lacked adequate internal controls** or that its structure favoured the commission of the offence of concealment of assets. In other words, **there was no evidence that the company's lack of preventive measures facilitated the criminal actions of the individuals**. The Supreme Court also emphasises that **the burden of proof lies with the prosecution, which must demonstrate not only that the legal entity failed to fulfil its supervisory duties, but also that this omission was serious and essential to the commission of the offence**.

Given that insufficient evidence was provided to indicate that the company facilitated the concealment of assets or that the organisational structure was deficient, the Court acquitted the company of criminal liability, concluding that **it had not been proven that the legal entity played an active role in the commission of the offence**.

In short, **both judgments mentioned in this Newsletter contravene the criteria of the previous Supreme Court Judgment, First Section, Judgment 298/2024, of 8th April, Rec. 6489/2021**, on the criminal liability of legal persons, which established the burden of alleging and proving the existence of a Compliance Programme in the defence. Therefore, **the current criterion regarding who bears the burden of proof concerns the prosecution**.

Case law

Order of the National Audience Court, Criminal Chamber, Section 2, 753/2025, of 10 December 2025, Rec. 598/2025

The ruling offers a particularly clear reminder of the legal limits of **criminal liability for legal persons** and the minimum requirements of criminality and factual specificity for a complaint to be admitted for processing.

The ruling analyses the appeal lodged against the order that refused to admit the complaint filed against three multinational pharmaceutical companies for alleged crimes of human gene manipulation (art. 159 of the Criminal Code), the use of genetic engineering to produce biological weapons (art. 160 of the Criminal Code) and crimes against public health (arts. 359 to 362 and 378 of the Criminal Code). The core of the judicial reasoning is forceful and clear: **not all crimes in the Criminal Code are susceptible to being committed by legal entities**, and the complaint does not pass this basic filter.

Firstly, the Court confirms that the offences under articles 159 and 160 of the Criminal Code cannot be committed by legal persons under Spanish criminal law. In response to the appellant's argument, which invoked article 162 of the Criminal Code, the Court recalls that this provision does not enable the attribution of criminal liability to legal persons, but merely allows, on an optional basis, the **imposition of additional penalties under article 129 of the Criminal Code** when the perpetrator of the offence is a natural person who is part of an organisation or company.

Secondly, with regard to crimes against public health, the Court acknowledges that **article 366 of the Criminal Code does contemplate the possible criminal liability of legal entities** for certain types of crimes. However, the complaint fails due to a complete lack of specificity: it does not identify the specific crime being charged, the specific facts that would constitute it, nor does it provide a minimum of evidence to support the charge. The Court is particularly clear in **rejecting the idea that criminal jurisdiction can serve as a channel for prospective investigations**, which are expressly prohibited in our system.

Other agreements and sanctioning resolutions on Compliance

MOLINS Compliance

- The AEPD received 19,000 complaints in 2024, with AI, data spaces and neurodata among its priority challenges.
- The AEPD does not allow hotels to photocopy ID cards or passports, with fines exceeding €10,000.
- Company fined €120,000 for revealing the identity of whistleblowers.
- Banca March faces a fine of €605,000 for breaching anti-money laundering regulations in a formal matter.
- Bank fined £28 million for failures in financial crime controls.
- The Tax Agency agrees to investigate neobanks for possible links to money laundering.
- BBVA ordered to compensate a customer who was the victim of phishing for her financial loss: €9,900.
- CNMC fines for hidden advertising.
- CNMV fines Deutsche Bank €10 million for infringements in the sale of currency derivatives.
- The CNMV fines Bestinver €100,000 for failing to provide 'clear and impartial' information about the characteristics of a product.
- The CNMC authorises a joint venture in the concrete sector, subject to certain commitments.
- Automatic reversal of sanctions against Iran: Council reinstates restrictive measures.
- AEPD fines Aena €10 million for its facial recognition system at airports.
- The CNMC (*S/0011/23, Eólica del Alfoz*) establishes for the first time the scope and duration of the prohibition on direct contracting in a sanctioning resolution.
- Fine imposed by the Anti-Fraud Office of Catalonia (OAC) on a company for retaliating against a whistleblower.

Other agreements and sanctioning resolutions on Compliance

MOLINS Compliance

The AEPD received 19,000 complaints in 2024, with AI, data spaces and neurodata among its priority challenges

The Spanish Data Protection Agency (hereinafter, AEPD) published its Annual Report for the 2024 financial year, which examines the **main emerging challenges in data protection**, as well as the most relevant **regulatory and statistical trends**, including the total volume of resolutions adopted.

During that year, the AEPD recorded 18,884 complaints, representing a 13% decrease compared to 2023, although the figures remain above the levels prior to that year. In terms of sanctions, 414 sanctioning and warning proceedings were concluded, of which 281 resulted in the imposition of financial penalties. The **five (5) sectors with the highest economic volume** of penalties were: the energy/water sector (which rose from €115,500 in 2023 to €11,680,600 in 2024); financial institutions/creditors (€5,356,900); Internet services (which rose to €4,547,380 compared to €1,058,700 in 2023); telecommunications (€3,330,000 compared to €1,942,000 in 2023) and fraudulent contracting (€2,538,200).

These five (5) sectors together accounted for 23% of the total amount of penalties imposed, which in 2024 amounted to €35,592,200.

The AEPD also recognises that the main challenge it faces is the use and development of AI and the analysis of its impact on data protection and fundamental rights.

The AEPD does not allow hotels to photocopy ID cards or passports, with fines exceeding €10,000

The AEPD has **clarified Royal Decree 933/2021**, which establishes the obligation for accommodation providers to collect certain data from their guests, arguing that this measure 'does not authorise them to request a copy of the customer's identity document', on the grounds that this would **violate the principle of data minimisation** and would constitute excessive processing of personal data.

To put an end to this practice, the **AEPD has been systematically sanctioning offenders in recent months** and years with fines of up to €15,000.

In addition, the AEPD extends this restriction to any other sector in which there is misuse or excessive use of the personal data of third parties with whom legal entities are associated.

We recall the recent sanction imposed on a crane company after an employee photographed a customer's ID card, resulting in a fine of €11,000.

Company fined €120,000 for revealing the identity of whistleblowers

The AEPD ordered a funeral home to pay €120,000 for failing to adequately guarantee the confidentiality of the personal data of several employees in relation to a case of workplace harassment and its resolution.

After the harassment protocol had been processed, the company sent a mass email with the resolution of the case, which included both the identity and job title of the five complainants. As a result of this communication, the entire company became aware of the events and the people who had been involved in them.

The AEPD considered that the funeral home **had violated article 5.1.f) of the GDPR by failing to adequately guarantee the confidentiality of the personal data collected under the harassment protocol**, and **fined it €200,000**, an amount that was reduced by 40% because the company acknowledged the error and paid within the voluntary period.

Banca March faces a fine of €605,000 for violating anti-money laundering regulations in a formal matter

At the end of January 2025, Banca March was fined €605,424 for violating anti-money laundering regulations. According to SEPBLAC, the fine was imposed due to **failures in the due diligence procedure** and in customer identification, which increased the risk of illegal transactions within the financial institution.

The entity has appealed SEPBLAC's decision before the Supreme Court, as it considers it to be a 'purely formal' error and defends its actions.

The controversy centres on the opening of an account for clients who had already been regularised by the Tax Agency and had been validated by it. Banca March accepted the deposit after formally checking its validation by the Tax Agency, but **without carrying out the enhanced due diligence measures** required by anti-money laundering legislation.

Other agreements and sanctioning resolutions on Compliance

MOLINS Compliance

Bank fined £28 million for failures in financial crime controls

The digital bank MONZO has been fined **£28 million** by the UK Financial Conduct Authority for serious failures in the prevention of money laundering and terrorist financing. It was found that the bank **had failed to implement adequate controls** for identifying and managing financial crime risks.

Similarly, the Luxembourg Financial Sector Supervisory Commission has fined the **Luxembourg subsidiary of the Allianz group £233,000** for failing to comply with its obligations to prevent money laundering and terrorist financing.

These sanctions reflect the **international trend towards strengthening due diligence** in the prevention of money laundering and terrorist financing. This is particularly true in a sector as important and exposed as the banking sector.

The Tax Agency agrees to investigate 'neobanks' for possible links to money laundering

The Tax Agency has announced an investigation into 'neobanks' with the aim of **identifying new methods of money laundering**. The less stringent regulation and anonymity of some of these new financial institutions have attracted the attention of the tax and fraud prevention authorities.

Therefore, there will be collaboration with the Financial Intelligence Unit and the Bank of Spain to **analyse suspicious patterns that may conceal fraudulent operations**.

It also warns that, if 'regulatory gaps' are detected, regulatory reform could be promoted to tighten the supervision and traceability requirements for these entities. All of this is **in line with European trends** and follows the recommendations of the European Banking Authority.

BBVA ordered to compensate a customer who was the victim of phishing for her financial loss: €9,900

The victim received an SMS embedded in the BBVA message thread informing her of an alleged unauthorised transaction, followed by a phone call from a person who falsely identified themselves as a bank employee.

The customer provided her credentials and security codes, under the false belief that the environment was legitimate.

Current Supreme Court doctrine establishes that, **except in cases of fraud or gross negligence on the part of the customer, the bank is liable for deficiencies in its security systems**. In addition, there is case law from the Provincial Court of Santander, which establishes that a user's conduct in the face of a well-crafted fraud attempt cannot be considered negligence if they act under distress and/or confusion.

The news highlights **the duty of care that banks must apply** in order to prevent fraudulent transactions and warns of the seriousness of security breaches that allow malicious third parties complete access to customer data.

CNMC fines for covert advertising

The National Commission for Markets and Competition (hereinafter CNMC) has recently fined several companies, including DAZN and Atresmedia, both for broadcasting covert advertising in their programming, with fines of **more than €180,000**.

Both sanctioned parties broadcast messages and advertising content without complying with the legal requirements for identifying and differentiating advertising. According to the General Audiovisual Communication Law, **advertising content must be clearly identified and differentiated from the rest of the programming**, requirements that both parties failed to comply with.

All penalties have been acknowledged and paid in advance in order to benefit from a reduction in their amounts.

This reinforces the objective of protecting viewers and consumers, highlighting the importance and obligation to clearly distinguish between editorial and advertising content.

CNMV fines Deutsche Bank €10 million for infringements in the sale of currency derivatives

The Spanish National Securities Market Commission (hereinafter, CNMV) has sanctioned Deutsche Bank for 'very serious' infringements in the marketing of currency derivatives, imposing a **fine of €10 million**.

In the resolution published in the Official State Gazette (BOE) on 29 January, the CNMV associates the sanction with a 'very serious' infringement of the obligation to provide information to clients to whom it provides investment services.

Other agreements and sanctioning resolutions on Compliance

MOLINS Compliance

In addition to the financial penalty, **the CNMV has also suspended, for a period of one year, investment advisory activities** relating to complex OTC (Over The Counter) derivatives that incorporate currency structures.

These disciplinary proceedings arose from an internal investigation by Deutsche Bank's parent company into its Spanish branch, which uncovered a series of malpractices that resulted in dismissals, compensation payments and, ultimately, the CNMV's sanction.

For the time being, the CNMV's decision has only become final in administrative proceedings, and Deutsche Bank has announced its intention to appeal the decision, confident in its internal processes and controls.

This case clearly illustrates **the importance of internal processes and controls in preventing non-compliance or irregularities** prior to criminal sanctions.

The CNMV fines Bestinver €100,000 for failing to provide 'clear and impartial' information about the characteristics of a product

The fund manager Bestinver Gestión, S.A., S.G.I.I.C. (hereinafter, Bestinver) has recently been sanctioned by the CNMV for failing to inform its clients in an 'impartial, clear and non-misleading' manner about the characteristics of one of its products, constituting a very serious infringement under article 284.1 of the Securities Market Law.

The aforementioned company has decided not to appeal the sanction through administrative channels, meaning that the sanction is now final.

Bestinver has publicly stated that it has cooperated fully with the CNMV's inspection and **has reviewed its procedures to prevent this from happening again**.

This sanction highlights the importance of **implementing and maintaining procedures** and protocols to prevent irregularities that could lead to sanctions.

The CNMC authorises a joint venture in the concrete sector, subject to certain commitments

Four companies in the same sector, Ribalta Pujol, Fiasa Mix, Calaf Grup and Gualtosal, have proposed to the CNMC the creation of a joint venture to manage and operate **15 ready-mixed concrete production plants**, thereby centralising a significant part of their production activity.

In reviewing the operation, the CNMC identifies as a key risk that the joint venture could be used as a **platform for the exchange of sensitive information** between **competing** companies in the concrete market and that, in some cases, also participate in related markets. This could also generate **risks of coordinated effects**, facilitating alignment in prices, commercial conditions or market strategies.

To neutralise this risk, the CNMC authorised the transaction subject to compliance with mandatory commitments:

- **Approve an internal competition protocol,** with operational measures on classification and confidentiality of information, rules on processing, definition of responsibilities and organisational safeguards to ensure separation between the Board and the Management Body and prevent interference by companies in day-to-day management; furthermore, its approval must be carried out within the established deadlines and **any modification requires the prior approval of the CNMC.**
- **Amend the Shareholders' Agreement:** formally incorporating these safeguards into the contractual framework governing the joint venture and reinforcing the independence and autonomy of the Management Body, including the figure of the Chief Executive Officer, as an essential element in preventing management from being influenced by the competitive interests of the parent companies.

In short, the CNMC points out that it does **not automatically review or validate** all the ancillary clauses of the agreement and that it is up to the companies to **self-assess** the competitive fit of these restrictions. The joint venture is permitted, but the resolution emphasises that business cooperation has **strict limits under competition law**, compliance with which is the direct responsibility of the companies involved.

Other agreements and sanctioning resolutions on Compliance

MOLINS Compliance

Automatic reversal of sanctions against Iran: Council reinstates restrictive measures

On 14th July 2015, Iran reached an agreement with the five permanent members of the United Nations Security Council (China, France, the Russian Federation, the United Kingdom and the United States), with Germany and with the support of the **EU High Representative**, on the **Joint Comprehensive Plan of Action (JCPOA),** aimed at ensuring that Iran's nuclear programme was exclusively for civilian and peaceful purposes. This agreement was endorsed by United Nations Security Council **Resolution 2231 (2015)**, which established the framework and timetable for **ending sanctions** related to nuclear activities, culminating on **16th January 2016**. In line with this, in October 2015 the EU adopted **Declaration 2015/C 345/01**, lifting European sanctions related to nuclear activities, while expressly maintaining the possibility of **reintroducing them in the event of significant breaches** by Iran.

On **28th August 2025**, France, Germany and the United Kingdom notified the United Nations Security Council that, in their view, Iran was in **significant non-compliance** with its commitments under the JCPOA. This notification triggered the '**snapback**' mechanism, which provides for the reintroduction of United Nations sanctions after a period of 30 days, unless the Security Council adopts a new resolution to prevent this. On **29th August 2025**, the EU High Representative, France and Germany submitted a joint recommendation to the Council urging the re-imposition of all EU nuclear sanctions that had been suspended or terminated. As no Security Council resolution was adopted, the sanctions regime was reinstated on **17th September 2025**, with the reintroduction of both United Nations sanctions (automatically transposed into EU law) and autonomous European measures.

Among the measures reintroduced are:

- **Travel ban** for certain individuals.
- **Freezing of assets** of designated individuals and entities.
- **Economic and financial sanctions** covering the commercial, financial and transport sectors.

AEPD fines Aena €10 million for its facial recognition system at airports

The AEPD has imposed a **fine of more than €10 million** on AENA for implementing a biometric identification system using facial recognition of passengers at eight Spanish airports, considering that this was **high-risk** data processing that was put into operation **without first carrying out a Data Protection Impact Assessment (DPIA)** in accordance with the terms required by the GDPR.

The ruling concludes that AENA carried out biometric processing operations aimed at uniquely identifying passengers to allow them access to certain airport areas **without adequately justifying the necessity and proportionality of the processing**. In particular, the AEPD emphasises that it was not demonstrated — either in the prior or subsequent analysis — that the use of biometrics was essential to achieve the intended purpose, especially when **less intrusive alternative means** capable of providing comparable levels of effectiveness and security existed.

The Agency acknowledges that the processing could be suitable for verifying identity and facilitating access control, but insists that the determining factor is proportionality, expressly described as a necessary and essential requirement.

The resolution also highlights that the system used was a one-to-many 1:N type, which from a data protection perspective implies an **active search within a set of pre-existing identities**, significantly increasing the level of risk, as it may more intensely affect the fundamental rights and freedoms of natural persons.

As a corrective measure, the AEPD imposes the **temporary suspension of all processing of biometric data** associated with this facial recognition system for passenger access control until AENA carries out a DPIA in accordance with the GDPR.

Other agreements and sanctioning resolutions on Compliance

MOLINS Compliance

The CNMC (S/0011/23, *Eólica del Alfoz*) establishes for the first time the scope and duration of the prohibition on direct contracting in its sanctioning resolution

The CNMC has sanctioned Eólica del Alfoz for abuse of a dominant position and, for the first time, specifies in the sanctioning resolution itself the scope and duration of the prohibition on contracting with the public sector, applying the criteria of Communication 1/2023 on **criteria for determining the prohibition on contracting due to distortion of competition**, for contraventions of Law 15/2007 on the Defence of Competition.

The infringement is based on the obstruction of access to an electrical connection point to a competitor, favouring a company in the same group. In addition to a fine of €958,593, a **prohibition on contracting** is imposed: (i) throughout the national territory; (ii) with the public sector entities mentioned in Article 3 of the LCSP, specifically covering works, supplies and services contracts relating to consulting, construction, operation, exploitation and maintenance of wind farms and their equipment; and (iii) for a period of **six months**, justified by the absence of direct impact on public procurement despite the seriousness of the infringement.

This case highlights the strategic importance of competition compliance programmes and protective measures as mechanisms for preventing or mitigating such consequences.

Fine imposed by the Anti-Fraud Office of Catalonia (OAC) on a company for retaliating against a whistleblower

The OAC has imposed a penalty on a company for the first time for retaliating against a whistleblower, in application of the **penalty regime linked to Law 2/2023**. The ruling affects Nora, S.A., a waste management company linked to the *Consell Comarcal de la Selva* and the Blanes Town Council, and results in a fine of €600,000 for committing a very serious offence.

The events date back to the end of 2022, when an employee requested internal information after suspecting possible irregularities related to hiring, bonus payments and time tracking. Among those who potentially benefited was the head of human resources, who went so far as to activate the internal harassment protocol against the whistleblower herself.

At the beginning of 2023, the worker reported the facts to the OAC and requested voluntary leave, but after approximately one month, the company imposed a disciplinary sanction of six days' suspension from work and pay.

This sanction was overturned by a Labour Court in Girona in December 2023, as it was deemed to be a **direct reprisal linked to the reporting of irregularities**, and the company was also ordered to pay compensation of €7,500. This decision was upheld by the High Court of Justice of Catalonia in July 2024, reinforcing the existence of a clear **causal link** between the disciplinary action and the employee's status as a whistleblower.

In view of these court rulings, the OAC initially proposed a fine of €800,000, which was finally reduced to **€600,000** after the hearing of arguments, maintaining the classification of the infringement as very serious.

Guidelines, institutional resolutions and reports of interest

MOLINS
Compliance

- ❑ Update of ISO 37001 on Anti-Bribery Management Systems.
- ❑ Update of UNE 19601 on Criminal Compliance Management Systems.
- ❑ New ISO 37003 on Fraud Management..
- ❑ New catalogues of indicators of money laundering and terrorist financing risk from the Commission for the Prevention of Money Laundering and Monetary Offences.
- ❑ 2025-2030 Strategic Plan of the Spanish Data Protection Agency. Responsible innovation and defending dignity in the digital age.
- ❑ State Plan to Combat Corruption of 9 July 2025.
- ❑ List of third countries posing a high risk of money laundering and terrorist financing.
- ❑ Resources for using AI.
- ❑ V Open Government Plan.

Guidelines, institutional resolutions and reports of interest

MOLINS Compliance

Update to ISO 37001 on Anti-Bribery Management Systems

On 28th February 2025, the International Organisation for Standardisation (hereinafter ISO) published the second edition of the ISO 37001 technical standard, a global benchmark in Anti-Bribery Management Systems, which introduces new features to strengthen alignment with other international standards and improve the effectiveness of compliance systems.

The most notable changes are:

- **Integration of climate change and compliance culture**: The impact of climate change must be considered in corruption risk analysis.
- **Strengthening the management of conflicts of interest**: Conflicts of interest are recognised as a key risk in the prevention of corruption and, along the same lines, the obligation to keep a register of declarations of conflicts of interest, with annual review, is introduced.
- **Review of key elements of the system**: Structural aspects of the Anti-Bribery Management System are updated, such as the due diligence procedure, internal audit, supervision and review of the system, as well as Compliance reporting.
- **Alignment with other ISO standards**: Adapted to maintain consistency with other ISO regulations, facilitating its integration into Global Management Systems.

Update to UNE 19601 on Criminal Compliance Management Systems

The UNE 19601 technical standard on Criminal Compliance Management Systems, initially published in 2017, was updated on 24 April 2025 by the Spanish Association for Standardisation. The most notable changes are as follows:

- **Strengthening the cultural approach to compliance**: This is adapted to the international definition of organisational culture as a sequence of values, ethics, beliefs and behaviours. The assessment of culture is now based on both objective evidence and the perception of stakeholders.
- **Clarification of criminal compliance objectives:** A distinction is made between specific, measurable objectives and the general statements that can be found in compliance policies.
- **Due diligence in investments:** It is clarified that due diligence processes do not apply to purely financial investments, delimiting their operational scope.
- **Training vs. awareness:** A distinction is made between internal technical training, aimed at members of the organisation, and awareness-raising activities, which also apply to business partners, with special attention to their autonomy.
- **Relocation of risk assessment:** The risk analysis exercise is moved from the planning chapter to the organisational context chapter, in line with technical standards ISO 19600:2014 and ISO 37301:2021.
- **Management of reporting channels:** Requirements are aligned with Law 2/2023 and ISO 37002, incorporating advanced measures to protect whistleblowers from retaliation and other harmful conduct, even when this results from negligence.
- **Governance and compliance function:** The core responsibilities of the compliance area are specified in relation to others that it must promote but does not directly control, following the distinction made in the ISO 37301 technical standard.
- **Harmonised ISO structure:** Although its use is not mandatory, the Spanish standard voluntarily chooses to follow the harmonised ISO structure, facilitating its integration with other management systems.

Guidelines, institutional resolutions and reports of interest

MOLINS Compliance

New ISO 37003 on Fraud Management

On May 29, 2025, the ISO 37003 technical standard was published, the **first specific international standard on Fraud Control Management Systems**. This standard is not certifiable, as it does not impose mandatory requirements, but rather offers recommendations for organizations that want to prevent, detect, and respond to fraudulent acts. ISO 37003 is also aimed at fraud that occurs within, from, or against the organization. Therefore, the content can be applied to entities of any size, sector, or legal nature, public or private, for-profit or non-profit, making it a useful and flexible tool for different organizational contexts.

The **main elements** of ISO 37003 are as follows:

- Analyze the **organizational context**, including internal and external factors that influence exposure to fraud.
- Ensure **leadership** commitment **and governance** by assigning responsibilities and coordinating between compliance, internal audit, and information security.
- **Plan and assess** fraud **risks**, identifying real threats and encouraging collaboration between areas.
- Provide **adequate resources** and promote integrity, differentiating between technical training and awareness-raising actions.
- Establish robust **preventive controls**, including policies on conflicts of interest, due diligence, and monitoring.
- Implement **effective** fraud **detection mechanisms** through the use of technological tools and reporting channels.
- Define an **organized response to fraud incidents** through evidence, reputational and legal impact management, as well as corrective and punitive actions.
- Evaluate the performance of the system periodically with **internal audits and reviews** to detect weaknesses.
- Apply a **continuous improvement** approach.

New catalogs of risk indicators for money laundering and terrorist financing from the Commission for the Prevention of Money Laundering and Monetary Offenses

In May, the Commission for the Prevention of Money Laundering and Monetary Offenses published new catalogs of risk indicators for nine groups of regulated entities, with the **aim of helping to improve the systems for the prevention of money laundering and terrorist financing** implemented by regulated entities and contributing to their effectiveness.

These catalogs summarize a **list of indicators of money laundering and terrorist financing risks**. The presence of these indicators in specific transactions does not necessarily imply the existence of illegal activity, but it can help the regulated entity identify cases to be selected for further examination.

The different indicators provided in these catalogs are adapted to the nature of the activity of each sector considered as a regulated entity, and are intended to help them develop their own catalogs, using these as a guide.

These catalogs **differ** in relation to: (i) the due diligence compliance process; (ii) specific transactions; (iii) beneficial ownership of assets; (iv) employees and agents of the regulated entity; and (v) possible links to criminal activities.

Guidelines, institutional resolutions and reports of interest

MOLINS Compliance

2025-2030 Strategic Plan of the Spanish Data Protection Agency. Responsible innovation and defending dignity in the digital age

On July 3rd 2025, the AEPD published its new **Strategic Plan 2025-2030, Responsible Innovation and the Defense of Dignity in the Digital Age**, which will set the course for the AEPD over the coming years, taking into account new technological, social, and geopolitical realities. The Strategic Plan defines eight guiding principles, in addition to 45 objectives structured around seven main areas.

- **Axis 1 – A smart agency:** The AEPD wants to improve efficiency through the strategic use of indicators and implement advanced monitoring systems supported by the adoption of an "AI first" policy.
- **Axis 2 – Technological innovation with guarantees:** The AEPD will monitor emerging technologies such as AI, biometric systems, and neurotechnologies, especially when they affect vulnerable groups.
- **Axis 3 – Promoting and supporting regulatory compliance:** The AEPD seeks to develop specific resources, such as technical kits, and update its guidelines tailored to the needs of different sectors.
- **Axis 4 – Promoting alliances and collaboration with professional entities:** The AEPD wants to strengthen cooperation with privacy professionals and will develop a cross-cutting intervention strategy aimed at vulnerable groups in the digital environment.
- **Axis 5 – International and national leadership and strategic influence:** The AEPD will strengthen its presence on the international stage by increasing its participation in the main national and international forums, especially the European Data Protection Board (hereinafter, EDPB).
- **Axis 6 – Effective and continuously improving administration:** The AEPD, as the AI Market Surveillance Authority, wants to increase its resources and optimize its organization through a comprehensive talent development and retention plan.
- **Axis 7 – Openness, proximity, and data protection culture:** The AEPD wants to improve its website by implementing tools and service channels to improve communication and active listening with professional sectors.

State Plan to Combat Corruption, July 9th 2025

On July 9, the government presented its State Plan to Combat Corruption, with the aim of consolidating a comprehensive and modern approach to this phenomenon. It is aligned with the recommendations of international organizations such as the Organization for Economic Cooperation and Development and the European Commission. The document is structured around **five pillars** of action:

The **first pillar** (risk prevention and strengthening of public controls) proposes as a key structural measure the creation of **an Independent Public Integrity Agency**, which would assume responsibilities that have hitherto been scattered across various areas, such as transparency, procurement control, fund supervision, and whistleblower protection. On the other hand, in the contractual sphere, a digital transformation of the current state portal is planned through the **use of AI** and **big data tools**, together with the **systematic implementation of** integrity **risk maps** in the management of public funds.

The **second** provides for a **significant extension of the guarantees offered to whistleblowers**. Despite the progress made by Law 2/2023, it is considered necessary to strengthen the protection of those who report irregularities, including those who do so directly to the Public Prosecutor's Office, police forces, or judicial authorities. It also provides for extending protection for a period of five years after the termination of whistleblowing channel managers, establishing the right to compensation proportional to the damage suffered, and requiring greater independence and effectiveness in the functioning of internal channels.

The **third** addresses the investigation and effective punishment of corrupt conduct. It calls for **strengthening the role of the Public Prosecutor's Office** in the **investigation** phase, as well as reforming the Criminal Code and judicial specialization in this area. From a Compliance perspective, three new developments stand out: (i) the legal requirement for Compliance systems for large operators; (ii) the imposition of financial penalties proportional to the illicit profit; and (iii) disqualification from contracting with the public sector in the event of convictions for corruption.

The **fourth** pillar reinforces the recovery of illicit assets, providing greater capabilities to the Asset Recovery and Management Office and proposing the possible incorporation of preventive administrative confiscation, following international models.

Finally, the Plan promotes a culture of integrity, with **mandatory training** for public officials and institutional campaigns that encourage the responsible use of reporting channels.

Guidelines, institutional resolutions and reports of interest

List of third countries posing a high risk of money laundering and terrorist financing

The Financial Action Task Force **(FATF) held its plenary meeting on October 24th 2025 in Paris**, adopting important decisions on **assessment, asset recovery, and emerging risks**. In the section on lists, it announced the **removal of Burkina Faso, Mozambique, Nigeria, and South Africa from the "gray list"** after they completed their action plans and demonstrated substantial improvements in the prevention and prosecution of money **laundering and terrorist financing**, while the **blacklist** remains **unchanged**. Although some progress has been recognized on the part of Iran, the FATF believes that conditions are not yet sufficient for its exclusion.

In this context, the **European Union** has updated its list of **high-risk jurisdictions for money laundering and terrorist financing**, reiterating that entities subject to the EU's anti-money laundering framework must apply **enhanced due diligence measures** to transactions involving these countries as a key tool for protecting the integrity of the EU financial system. This update **includes Algeria, Angola, Ivory Coast, Kenya, Laos, Lebanon, Monaco, Namibia, Nepal, Venezuela, Bolivia, Russia, and the British Virgin Islands**, and **removes**. **Barbados, Gibraltar, Jamaica, Panama, the Philippines, Senegal, Uganda, the United Arab Emirates, Burkina Faso, Mozambique, Nigeria, South Africa, Mali, and Tanzania.**

The European Commission emphasizes that the list is aligned with the work of the **FATF** and its enhanced supervision methodology. However, there has not yet been an official publication of the list.

Resources for the use of AI

The **Spanish Agency for the Supervision of Artificial Intelligence** (hereinafter AESIA) is the public body responsible for **ensuring the ethical and safe use of AI in Spain**. On December 10, 2025, this body published various guidelines developed within the framework of the **Spanish pilot project for the AI regulatory sandbox** (the term sandbox refers to a supervised testing space where new AI solutions can be tested in a controlled and safe manner before being applied on a large scale).

The purpose of these guidelines is to provide a practical support framework to facilitate the implementation and compliance with the obligations set out in the European AI regulations.

It should be noted that, although these guides **are not binding documents and do not replace or develop the content of the Regulation**, they do provide guidance and recommendations consistent with regulatory requirements, which are particularly useful until the harmonized standards to be applied uniformly in all Member States are approved.

These guides are **dynamic documents**, subject to a continuous process of review and improvement, which will evolve in line with the development of technical standards and guidelines published by the European Commission.

A **total of 17 documents** have been developed, organized into the following blocks:

- **Introductory guides:** guides 1 and 2. These provide a general understanding of the AI Regulation from a theoretical and practical point of view.
- **Technical guides:** guides 3 to 15. Each of these thirteen (13) guides provides operational guidance on translating the requirements of the AI Regulation into concrete measures, facilitating the design, implementation, and documentation of AI systems.
- **Checklist user manual:** guide 16. Explains, in a practical way, **how to use the checklists to self-assess the compliance** of an AI system with the requirements of the AI Regulation and **plan the necessary measures** to correct any shortcomings.
- **Checklist compendium and examples in zip file.** Brings together, in a downloadable format, **checklists and practical models** to facilitate their direct application, support internal documentation, and standardize compliance assessment in AI projects.

Guidelines, institutional resolutions and reports of interest

MOLINS Compliance

V Open Government Plan

The **V Open Government Plan 2025–2029**, in force since **6th October 2025**, consolidates a significant shift in the **public sector's integrity and compliance** agenda, moving from primarily declarative approaches to a framework with structured, **measurable measures designed for effective implementation**. The Plan is structured around ten commitments, with **Commitment 3: Integrity and Accountability** standing out in terms of compliance. It incorporates **24 initiatives** aimed at strengthening public confidence through **integrity maps, conflict of interest prevention, interest group (lobby) regulation, accountability and corruption prevention**, including initiatives derived from the **State Plan to Combat Corruption**.

Within this framework, the Plan expressly promotes the **Integrity System of the General State Administration (SIAGE)** —approved by Agreement of the Council of Ministers on 28 January 2025—, which is now established as a **methodological and operational reference** for extending integrity systems to the entire public sector. Among the most relevant lines of action are: (i) the extension of **integrity risk maps and matrices** to the entire Administration, aligned with the **OECD Public Integrity Framework** and with a special focus on **public procurement**, incorporating **early warning mechanisms ('red flags')**; (ii) the **diagnosis of SIAGE maturity** to identify strengths and areas for improvement; (iii) the promotion of **regulatory compliance programmes in the AGE** as an essential preventive tool, with the explicit intention that the model be **replicable** and act as an **institutional reference**; and (iv) the incorporation of cultural measurement instruments, such as **ethical climate surveys**, to assess the real impact of the system on the organisation.

Likewise, Commitment 3 incorporates initiatives with strong transformative potential in terms of integrity: the development of a **National Anti-Fraud Strategy**; the processing of the **Draft Organic Law on Public Integrity** (with measures to strengthen public procurement and tougher penalties for corruption); the possible creation of an **Independent Public Integrity Agency** with supervisory, risk assessment and investigative functions; the design of a **comprehensive whistleblower protection system**; and the transformation of the **Public Sector Procurement Platform** through **Big Data and artificial intelligence** to detect irregular patterns and evolve towards structural and automated supervision. All of this is accompanied by a specific focus on a **culture of integrity**, with dissemination and mandatory training for public employees and senior officials.

The **key idea from a Compliance perspective** should be that Plan V reinforces an emerging standard in the public sector: integrity is managed as a **compliance system**, based on **risk**, with verifiable controls, maturity metrics, preventive tools and accountability mechanisms.

Compliance Department publications (January-December 2025)

MOLINS Compliance

- Another step towards protecting whistleblowers: the creation of the Independent Whistleblower Protection Authority of the Community of Madrid.
- How is SEPBLAC transforming the fight against money laundering and terrorist financing?
- New edition of ISO 37001: key changes and transition period.
- Molins Compliance: strategy, prevention and trust.
- The new version of UNE 19601: an effective response to the challenges of good governance in organisations.
- Corruption under scrutiny: key points of the new State Plan to fight corruption.
- ComplianceKeys#25: The origins of Compliance in Spain.
- ComplianceKeys#26: Compliance, business ethics and organisational culture.
- ComplianceKeys#27. How does compliance affect a company's reputation?
- Crime committed by a legal entity: new change in criteria by the Supreme Court (STS 768/2025 of 25 September and 836/2025 of 14 October) on proving the ineffectiveness of Compliance.
- ComplianceKeys#28. Compliance in the public sector: integrity and good governance as pillars of public management.
- ComplianceKeys#29. Compliance and Sustainability.
- ComplianceKeys#30. Compliance and money laundering.

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