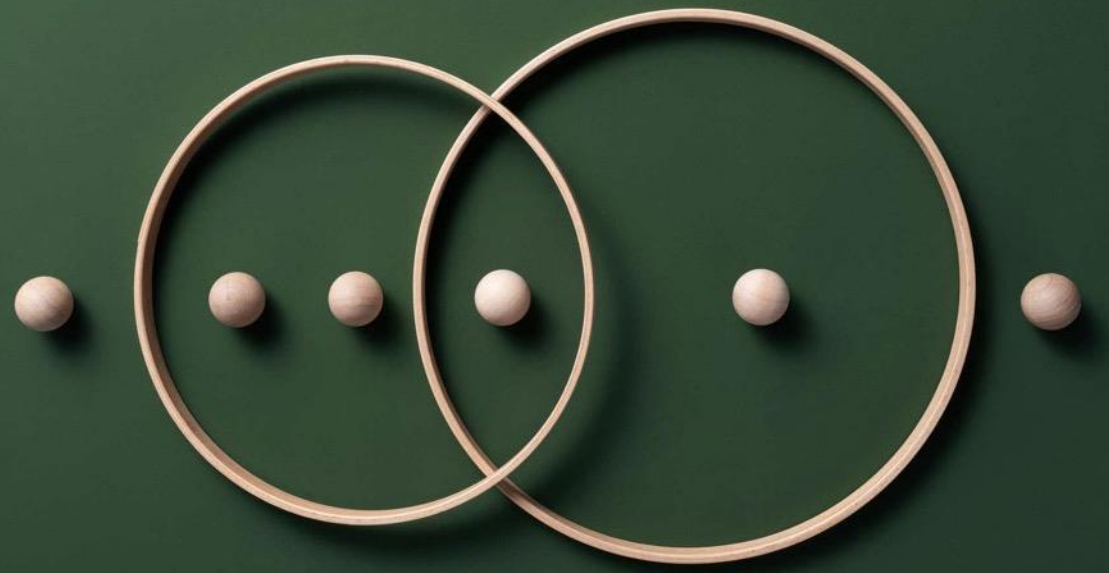
COMPLIANCE &
INVESTIGATIONS

CUATRECASAS COMPLIANCE CORNER

2ND EDITION. JULY 2025



CUATRECASAS

Contents

2nd Edition. July 2025

CUATRECASAS

1. Regulatory developments

- New UNE 19601:2025 on criminal compliance management systems
- International sanctions affecting Syria and Russia
- Entry into force of Accessibility Act in Spain: Key aspects
- GDPR amendments for SMEs and mid-caps
- Artificial intelligence developments: FAQs and obligations for high-risk systems
- CNMC Guidelines for public tenders
- Act 2/2025 on permanent incapacity and contract termination
- Adoption of sustainable mobility plans in Catalonia
- Restrictions on Chinese medical devices in EU tenders
- Omnibus I Proposal on corporate due diligence in the European Union

2. Good to know

- Overview of main ISO/UNE standards currently in force or under development
- Updates from the Spanish Data Protection Agency
- Release of new Data Security Program Compliance Guide for the U.S. Data Security Program
- CNMC Guide on compliance programs
- Transposition of EU Directive 2023/970, establishing obligations for justifying and reviewing salary policies

3. Relevant cases

- Supreme Court ruling on the criminal liability of legal entities
- Analysis of an investigated party's right to refuse testimony under Act 2/2023
- First fines imposed under Digital Markets Act
- Evidence obtained through private investigators and workplace monitoring

4. Beyond our borders: International trends and developments

- U.S.: New DOJ Guidelines for Investigations and Enforcement of the Foreign Corrupt Practices Act (FCPA)
- Peru: First conviction under the corporate administrative liability regime for criminal offenses
- Mexico: Proposed amendments to the Federal Economic Competition Act
- Colombia: New anti-money laundering obligations for transportation companies

5. Cuatrecasas events

- Past events and resources
- Upcoming events: Annual Compliance & Investigations Day - 2nd edition

6. Editorial team

1. Regulatory developments

1 REGULATORY DEVELOPMENTS

New UNE 19601:2025: Key developments in criminal compliance management systems (1)

In April of this year, the long-awaited update of UNE 19601:2025 Standard was published, consolidating its position as the benchmark standard in Spain for implementing, evaluating and certifying criminal compliance management systems.

This update responds to the evolution of the national legal framework, practical experience gained since 2017, and the need to align with the latest international standards, such as ISO 37301:2021 (Compliance Management Systems) and ISO 37002:2021 (Whistleblowing Management Systems).

MAIN DEVELOPMENTS

- **Regulatory updates and international harmonization**: The new version incorporates recent reforms to the Spanish Criminal Code and aligns with international standards. It adopts the harmonized structure (HLS), facilitating integration with other management systems (e.g., general compliance and anti-bribery).
- **Conceptual clarity in training and awareness**: It explicitly distinguishes between training (developing skills for specific functions) and awareness (general awareness). This allows for the design of more effective programs tailored to each group's exposure to criminal risk, including business partners.
- **Strengthening the compliance function and the organizational culture**: The revised standard better defines direct responsibilities of the compliance area versus those it should promote but whose results it cannot guarantee. It also strengthens the role of the criminal compliance body by requiring independence, authority and access to decision-making entities. The compliance culture is defined along the sequence "Values/Ethics/Beliefs/Behaviors," with evaluations combining indicative approaches and stakeholder perceptions.
- **Risk management and evaluation**: Criminal risk assessments have been moved to the "Context of the organization" section, aligning with ISO standards and emphasizing the regularity and updating of this process.
- **Internal reporting channels**: The update places special emphasis on the importance of implementing effective, secure and confidential whistleblowing channels, in line with Directive (EU) 2019/1937, Act 2/2023 and ISO 37002: 2021. Protection of whistleblowers is expanded to protect them from any harmful conduct, not only reprisals. It also provides for whistleblowing by legal entities.

1 REGULATORY DEVELOPMENTS

New UNE 19601:2025: Key developments in criminal compliance management systems (2)

- **Due diligence and financial oversight**: The update clarifies the treatment of financial investments lacking management control and strengthens due diligence criteria for positions particularly exposed to criminal risks.
- **Governance and goal setting:** The standard distinguishes between criminal compliance objectives and the framework for establishing them, ensuring they are not confused with programmatic statements. The objectives set for each period must be documented separately.
- **Flexibility and national adaptation:** Although the standard follows the ISO structure, certain content has been adjusted to reflect the Spanish context. For example, references to climate change present in the international harmonized structure are omitted.

UNE 19601:2025 marks a significant step towards more professionalized, integrated and internationally aligned criminal compliance. It reinforces the need for a strong ethical culture, the effectiveness of internal controls, and the accountability of senior management and the compliance body. Its adoption and certification are consolidated as key components in preventing criminal risks and safeguarding the reputational integrity of organizations in Spain.

1 REGULATORY DEVELOPMENTS

Developments in international sanctions

ECONOMIC SANCTIONS ON SYRIA LIFTED

- On May 28, 2025, the European Union (“**EU**”) lifted the economic sanctions that had been imposed on Syria, except those grounded in security concerns.
- Subsequently, on June 30, 2025, U.S. President Donald Trump signed an executive order lifting most economic sanctions against Syria, effective July 1, 2025. However, this measure excludes certain individuals from the sanctions relief.

UPDATES ON SANCTIONS AGAINST RUSSIA

- In April 2025, the U.S. Congress introduced a bill proposing new sanctions on Russia. Currently under parliamentary discussion, the bill contemplates primary and secondary sanctions on Russian banks and a 500% tariff on countries purchasing Russian energy.
- On May 20, 2025, the EU approved its 17th sanctions package against Russia. The new measures include (i) additional sanctions targeting individuals and entities; (ii) prohibition of access to ports and services related to maritime transport for vessels within Russia's clandestine fleet; (iii) export restrictions on dual-use goods and technologies for new entities, some located in third countries; and (iv) new restrictions on the export of goods that contribute to Russia's military and technological advancements, such as chemical precursors for energy materials and spare parts for machine tools.
- On June 16, 2025, the EU extended for another year the sanctions it initially adopted in response to Russia's illegal annexation of Crimea and Sevastopol.
- On June 17, 2025, the EU imposed new tariffs on agricultural products and fertilizers from Russia and Belarus, as part of its strategy to intensify economic pressure on both countries.
- Also, in June 2024, the EU proposed its 18th sanctions package focused primarily on the oil and banking sectors. However, this package is blocked due to a lack of consensus among Member States, particularly due to opposition from Hungary and Slovakia.

1 REGULATORY DEVELOPMENTS

Entry into force of the Accessibility Act in Spain: Key aspects

On June 28, 2025, Act 11/2023 on accessibility ("**Accessibility Act**"), which transposes Directive 2019/882, entered into force. The Accessibility Act applies to all organizations falling within its scope (article 2), regardless of their size or legal structure, provided the affected products or services are offered in the domestic market.

Affected products and services

The Accessibility Act applies, among others, to consumer-use general-purpose computer equipment, operating systems for this equipment, certain self-service terminals such as payment terminals, self-service terminals dedicated to service provision, and electronic readers. It also applies to certain services, such as consumer banking services and e-commerce services.

Compliance obligations

- Review and adaptation: Ensure affected products and services comply with the universal accessibility requirements outlined in Annex I to the Accessibility Act.
- Accessibility declaration: Prepare and maintain an accessibility declaration detailing the compliance level of these products and services.
- Staff training: Provide adequate and ongoing training to employees of service providers concerning information delivery, advisory services, advertising, and diversity-oriented support.

Failure to comply with the Accessibility Act is sanctioned in accordance with specific sectoral legislation, and subsidiarily, under the General Law on the Rights of Persons with Disabilities and their Social Inclusion, which establishes fines of up to €90,000. See more.

GDPR amendments for SMEs and mid-caps

The European Commission has presented its fourth Omnibus package, revising the General Data Protection Regulation ("**GDPR**") to ease administrative requirements for small and medium-sized enterprises ("**SMEs**") and mid-caps, which did not previously receive differentiated treatment.

A key reform raises the employee threshold from 250 to 750 for exemption from maintaining records of processing activities. The package also promotes codes of conduct and sectoral certification schemes tailored to the size and capacity of SMEs and mid-caps.

These changes uphold the GDPR's protective intent while simplifying compliance for smaller companies. After the public consultation phase, the revised text is expected to enter into force during the second half of 2026, accompanied by a transitional period to facilitate the gradual adaptation for authorities and organizations. See more.

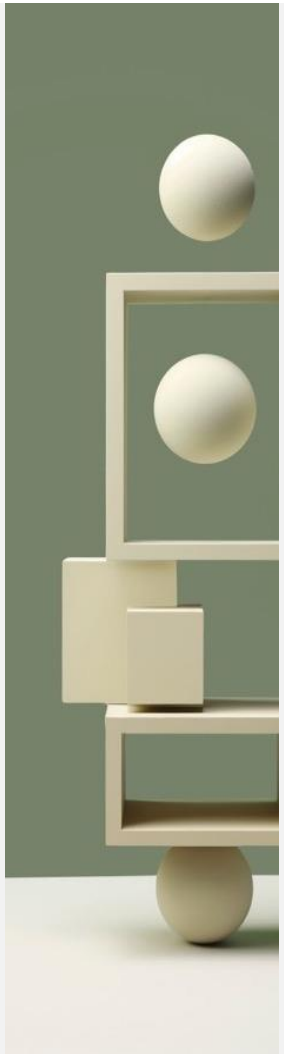
1 REGULATORY DEVELOPMENTS

Artificial intelligence developments: FAQs and obligations for high-risk systems

The European Commission has published an FAQ document detailing the scope of Article 4 of Regulation (EU) 2024/1689 on the obligation of "AI literacy." According to this document, all individuals interacting with AI systems, including employees, must have a "sufficient level of literacy" in technical, legal, ethical, and governance aspects. However, these individuals do not need formal certifications, and a specific manager does not need to be appointed for this purpose. From February 2, 2025, companies must internally document all training activities related to AI literacy. To support these efforts, the European AI Office has launched a live repository compiling real-world examples of AI literacy initiatives contributed by companies that are signatories to the AI Pact. This repository is aimed at facilitating the exchange of training models.

Starting August 2, 2025, providers and parties deploying high-risk AI systems must implement robust governance schemes, such as (i) introducing quality management procedures and automatic record keeping, (ii) subjecting AI systems to conformity assessments and affixing the CE mark of compliance, and (iii) registering AI systems in the Community database. See more

To ensure adaptation to these requirements, compliance programs can incorporate the following strategies: carry out periodic risk analyses tailored to specific use cases, develop internal policies to promote an ethical and transparent organizational culture, implement periodic AI-focused training for employees, clearly define roles and responsibilities within governance structures, and incorporate continuous auditing tools and early-warning systems.



CNMC Guidelines for public tenders

The National Commission for Markets and Competition ("**CNMC")** has published a new practical guide focused on preparing and designing public tenders (the "**Guide**"). Its aim is to promote competition, minimize collusion risks and improve the efficiency of public spending. This marks the third phase of the update to the CNMC's Guide on Government Procurement and Competition.

The document includes methodologies for market research, the use of AI, and preliminary consultations. It also includes specific recommendations to facilitate the participation of SMEs. It introduces strategies to avoid technological capture while strengthening social and environmental clauses, in addition to offering a practical self-assessment checklist.

The CNMC emphasizes that tenders must be designed with objectivity, technical justification and effective monitoring in mind. Also, they should adhere not only to procurement regulations but also to the principles of good governance and sound regulation.

1 REGULATORY DEVELOPMENTS

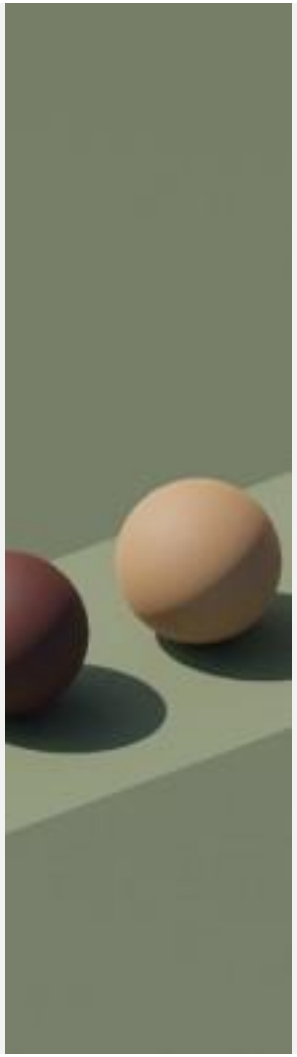
Act 2/2025 on permanent incapacity and contract termination

To align contract termination with international regulations and the caselaw of the Court of Justice of the European Union ("**CJEU")**, Act 2/2025 requires companies to take appropriate measures to preserve the employment of individuals considered as being in a situation of permanent incapacity, unless these adjustments are not feasible because they are excessively burdensome for the company.

This new regulation eliminates the option of automatic termination of employment contracts in cases of permanent incapacity, directly impacting company policies concerning occupational health and safety, as well as diversity and inclusion policies. Failure to comply with this obligation may constitute discrimination based on illness.

Adoption of sustainable mobility plans in Catalonia

Before August 9, 2025, workplaces employing over 500 employees (or 250 per shift), as well as centers with over 200 employees located in areas with severe pollution, must implement a sustainable mobility plan. This plan, which must be developed in collaboration with the employees' legal representatives, aims to reduce pollution and promote sustainable transportation, in accordance with Decree 132/2024, of July 30. See more.



Restrictions on Chinese medical devices in EU tenders

The European Commission has adopted Implementing Regulation (EU) 2025/1197, restricting the participation of companies and medical devices originating in the People's Republic of China ("**PRC**") in public tenders within the EU. Since June 30, 2025, this implementing regulation excludes bids from PRC operators in public tenders for medical devices exceeding €5 million in value and caps the proportion of inputs originating from the PRC at 50% for bids submitted by companies from other countries.

This marks the first application of restrictions under Regulation (EU) 2022/1031, also known as the "International Procurement Instrument." These measures were introduced following an investigation by the European Commission into the challenges faced by European companies in accessing China's public procurement market in the healthcare sector. See more.

1 REGULATORY DEVELOPMENTS

Omnibus I proposal on corporate due diligence in the EU

Where are we?

The European Commission has initiated a review of the main corporate sustainability standards, including the Corporate Sustainability Reporting Directive (**"CSRD"**), the Corporate Sustainability Due Diligence Directive (**"CSDDD"**) and the EU Taxonomy Regulation.

This review, driven by the Omnibus I Opposition Resolution submitted in February 2025, aims to reduce the administrative burden for companies while enhancing their competitiveness. However, the revision process maintains commitments to decarbonization goals and adherence to the double materiality principle in managing environmental and social risks and impacts.

Currently, both the CSRD and the CSDDD have been approved and enacted; however, their implementation has been postponed by Directive (EU) 2025/794 ("Stop the Clock"). This directive allows more time for companies and Member States to adapt while the legislative review process is underway. See more.

Subsequently, the Council of the European Union agreed on its position for reforming the CSRD and the CSDDD, focusing on reducing the administrative burden and mitigating cascading effects on SMEs. The Presidency is now prepared to enter negotiations with the European Parliament after it formulates its own negotiating position, with the overall goal of reaching an agreement on this dossier.

2. Good to know

2 GOOD TO KNOW

Overview of main ISO/UNE standards currently in force

The compliance regulatory environment is supported by a set of international ("**ISO")** and national ("**UNE")** standards that establish requirements and best practices for ethical management, risk prevention and organizational governance.

Currently, the most established and widely adopted UNE and ISO standards include the following:

- **ISO 37301:2021: Compliance management systems.** Sets requirements for establishing, maintaining and continuously improving an effective compliance management system, applicable to organizations of any size or type.
- **ISO 37001:2025: Anti-bribery management systems.** Provides a framework for preventing, detecting and addressing bribery while strengthening integrity and transparency within organizations.
- **ISO 37002:2021: Guidelines for managing whistleblowing channels**. Offers recommendations for implementing and managing internal whistleblowing systems, promoting whistleblower protection and a culture of integrity.
- **UNE 19601:2025**: **Criminal compliance management systems**. Serves as a benchmark standard in Spain for implementing, evaluating and certifying criminal compliance management systems. It incorporates recent legal reforms, aligns with international standards and strengthens the independence, authority and access of the criminal compliance body. It also promotes whistleblower protection and an ethical organizational culture.
- **UNE 19602: 2019: Tax compliance management systems.** Establishes requirements and guidelines for implementing a management system aimed at preventing and detecting tax-related risks. It fosters compliance with tax obligations and ensures transparency in dealing with the tax authorities.
- **UNE 19603: 2023: Competition compliance management systems.** Provides a framework for preventing, detecting and managing risks associated with antitrust regulations. It encourages free competition and promotes integrity in business relationships.

2 GOOD TO KNOW

Future ISO/UNE standards

In addition to the existing ISO standards, new standards are being developed to extend the scope and specialization of compliance management systems. Key standards currently in development include the following:

- **ISO 37003: Fraud control management systems.** Provides a specific framework for preventing, detecting and responding to fraudulent activities.
- **ISO 37302: Guidelines for measuring the effectiveness of compliance systems.** Facilitates the objective evaluation and continuous improvement of compliance programs.
- **ISO 37303: Compliance competencies.** Defines the knowledge, skills and attitudes required for professionals in the compliance area.
- **ISO 37200: Combatting human trafficking and forced labour.** Provides organizations with tools to identify, prevent and manage risks associated with human trafficking and forced labor.
- **ISO 37401: Diversity management from governance.** Encourages the creation of inclusive and equitable environments through effective governance practices.
- **ISO 37201: Prevention of violence against women in organizations. E**stablishes measures and controls to eradicate gender-based violence within organizational contexts.
- **ISO 37009: Conflict of interest management.** Provides a framework for identifying, preventing and managing conflicts of interest, ensuring integrity in decision-making processes.

The integration of these standards, both those already in force and those being developed, enables organizations to create more robust compliance systems that are aligned with international best practices and adapted to new regulatory and social challenges.

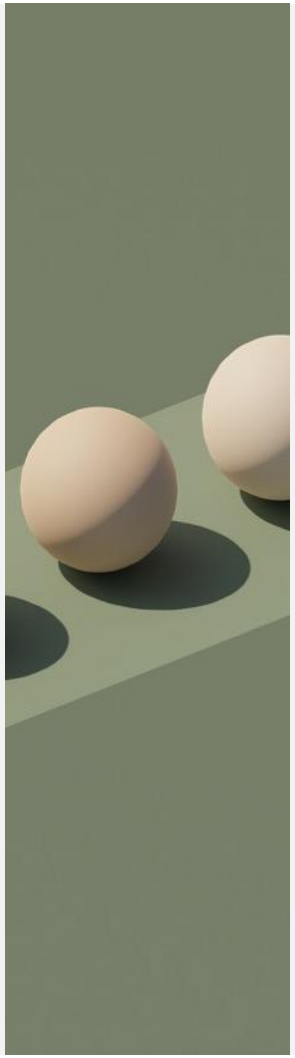
Staying up to date with these standards is essential to anticipate risks, reinforce an ethical organizational culture and consolidate corporate reputation.

2 GOOD TO KNOW

Updates from the Spanish Data Protection Agency (AEPD)

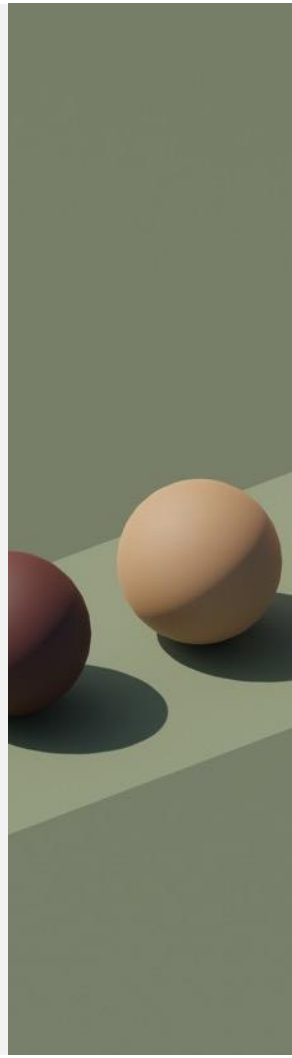
- **Who is currently head of the AEPD?** In March 2025, Lorenzo Cotino Hueso and Francisco Pérez Bes assumed their positions as president and deputy of the AEPD, respectively. During their opening speeches, they both emphasized the need to strengthen the agency's proactive stance on challenges related to AI, data spaces and the protection of children in the digital environment.

- **AEPD's strategic line of action:** The agency has published its Strategic Plan 2025–2030, which is built on eight guiding principles, of which we highlight (i) intelligent supervision to anticipate and address emerging risks; and (ii) technological innovation, establishing a Privacy and Technology Laboratory in collaboration with universities and other European authorities. The plan also outlines seven key areas of action, such as (i) strategic cooperation at the national and international levels; (ii) compliance support, with a focus on SMEs; (iii) internal digital transformation; and (iv) a more open and accessible agency,.



- **What does the** AEPD's 2024 annual report include? The report reflects a year of significant activity. Key highlights include the deployment of tools and guidelines for protecting minors in digital environments, the AEPD's preparation for its potential designation as the Market Surveillance Authority for the AI Regulation, and efforts to streamline data breach management through automation, enhancing operational efficiency. The report also covers international collaboration projects in areas such as neurodata, genetic data and blockchain. Also noteworthy is the fact that the AEPD managed 19,722 claims during the past fiscal year, marking the second-highest figure in its history.

- **What new section has the AEPD added to its website?** The AEPD introduced a new section dedicated to the most legally or socially significant criteria that it follows in its resolutions. This initiative aims to provide an additional channel for communication and engagement with citizens, data controllers, data protection professionals, and the media, offering useful and accessible information. Currently, the section includes the agency's positions on topics such as the processing of personal data of self-employed individuals, the processing of biometric data with AI in online university assessments, and whether AI systems should comprehend the exercise of data protection rights.



2 GOOD TO KNOW

Release of new Data Security Program Compliance Guide for the U.S. Data Security Program

- **Why should U.S. companies review their crossborder data transfers?** U.S. companies should carry out this review due to escalating geopolitical tensions and new regulations from the Department of Justice, such as the Data Security Program ("**DSP**"). These regulations impose stricter controls on the transfer of sensitive or government-related data outside the country.
- **What types of data are subject to the new DSP regime?** The DSP encompasses not only sensitive personal data (such as financial or health information) in large volumes, but also technical data related to R+D or patents. This significantly broadens the scope of regulatory control.
- **When did the DSP fully take effect?** The DSP was fully implemented on July 8, 2025. Before that date, a 90-day grace period allowed companies to demonstrate good-faith compliance efforts. However, after this period, companies are expected to fully adapt to the changes or face potential sanctions.
- **What penalties can companies face for non-compliance with the DSP?** Companies may face fines of up to USD 366,000 (or double the value of the transaction) and severe criminal penalties, including prison sentences of up to 20 years and multi-million-dollar fines, particularly in cases of serious non-compliance.
- **What role does the Data Security Program Compliance Guide play in DSP compliance?** The Data Security Program Compliance Guide, published by the National Security Division on April 11, 2025, outlines best practices for implementing the DSP. These include adopting certain contractual clauses, conducting audits and implementing other internal controls. The guide helps companies design robust DSP compliance programs and simplifies the process of demonstrating proper practices during inspections.

2 GOOD TO KNOW

CNMC Guide on compliance programs

EVALUATION TO DATE AND FUTURE EXPECTATIONS

Last month marked the fifth anniversary of the publication of the "Guide on compliance programs in relation to antitrust rules" (the "Compliance Guide") by the CNMC. Over the past five years, the Compliance Guide has become the main compliance standard for evaluating the effectiveness of compliance programs in this area in Spain, serving as a reference for both the CNMC and other authorities and public administrations.

Our previously published Legal Flash describes the effectiveness criteria outlined in the CNMC's Compliance Guide, as well as the multi-level benefits stemming from the successful development of a compliance program in the antitrust field. It also reviews the key aspects of the practical application of the Compliance Guide since it was adopted, along with judicial precedents that have emerged to date, which indicate a high standard for the operation and effectiveness of such programs.

For further details on the fundamental aspects and key features of compliance programs in defense of competition, click here.

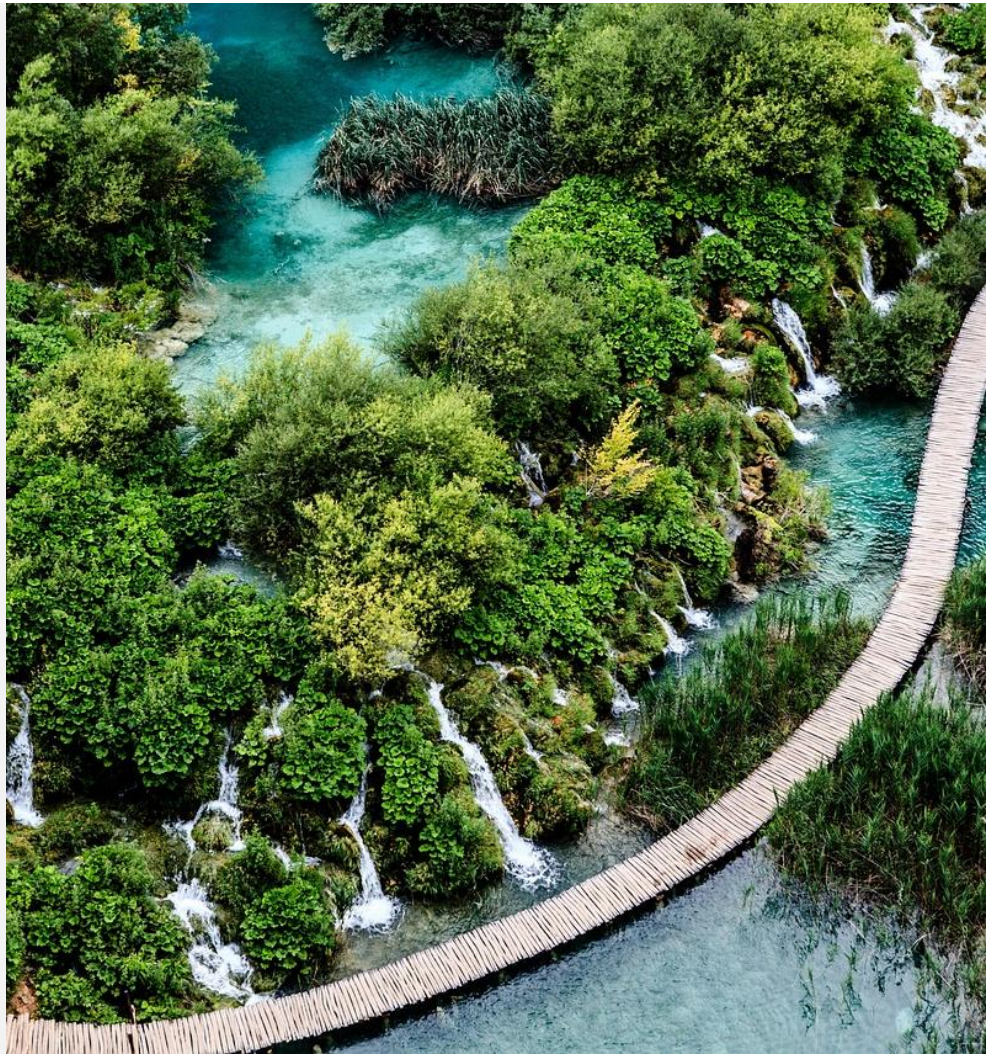
2 GOOD TO KNOW

Transposition of EU Directive 2023/970, establishing obligations for justifying and reviewing salary policies

On June 7, 2026, the transposition period for EU Directive 2023/970 on pay transparency will end, imposing new obligations on organizations. Among the requirements are justifying pay gaps exceeding 5% between women and men within the same job category and providing employees with access to the criteria used to determine their remuneration, salary levels and progression.

Previously, justification was required for pay gaps starting at 25%, making this lowered threshold a significant change for organizations. Specifically, this adjustment may result in a notable increase in costs.

Accordingly, in addition to the specific transposition terms of EU Directive 2023/970 into national legislation, companies must carry out an in-depth review of their salary policies and remuneration levels to comply with these new requirements.



3. Relevant cases

3 RELEVANT CASES

Supreme Court ruling on the criminal liability of legal entities

The Supreme Court, in its ruling 372/2025 of April 11, 2025, establishes a new benchmark in attributing criminal liability to legal entities. Specifically, it confirms that demonstrating a structural defect in the company's management, oversight or supervisory systems is essential for convicting the organization.

In this ruling, the Supreme Court acquitted a company previously convicted of fraud, emphasizing that the mere fact of a manager committing a crime is insufficient to automatically hold the company liable.

The ruling highlights that legal entities are entitled to the same procedural rights and guarantees as natural persons. Consequently, to convict a company, the prosecution must provide specific and detailed evidence of failures in prevention plans or internal controls, instead of relying solely on the director's actions.

The Supreme Court explicitly rejects the notion of a "rebuttable presumption" of organizational failure merely because an employee or manager committed a crime. Rather, it establishes that if the proven facts do not describe a failure of prevention plans or organizational defects, the company must be acquitted.

This ruling underscores the importance of having effective and fully implemented criminal compliance systems that go beyond mere "paper compliance." It is essential to demonstrate their practical application and the presence of a culture of compliance within the organization.

In short, the ruling raises the evidentiary and diligence standards required of companies and provides an additional guarantee of legal certainty to those managing regulatory compliance.

Key takeaway: A company's criminal liability must be based on specific and proven facts, not automatic assumptions.

3 RELEVANT CASES

Analysis of an investigated party's right to refuse testimony under Act 2/2023

In its ruling 704/2025 of June 4, 2025, the Supreme Court affirmed that while individuals summoned during preliminary investigations (informative proceedings preceding disciplinary proceedings) have a duty to appear if summoned, this duty must be balanced with the constitutional right against self-incrimination.

The duty to cooperate must be weighed against the constitutional right not to testify against oneself, particularly when incriminating questions are posed to a person clearly identified as a potential subject of the investigation. In these cases, this right extends to this preliminary phase, meaning individuals' right to refuse to answer questions that could lead to self-incrimination is protected by the Constitution, even before the formal initiation of a sanctioning procedure.

Although the ruling pertains to a specific case within the civil service, its doctrine is highly relevant for internal investigations in the private sector, especially under Act 2/2023. This act governs internal information systems and establishes the duty of collaboration under article 19 and the potential sanctions for lack of collaboration under article 63. This caselaw requires that these obligations be interpreted and applied with respect for the fundamental right against self-incrimination. Consequently, refusing testimony can be fully justified if there is a genuine risk of self-incrimination and the individual is clearly identified as a subject of the investigation.

The Supreme Court's ruling highlights the importance of strengthening guarantees in internal investigation processes, revising protocols and providing training to ensure the fundamental rights of investigated individuals are respected. Therefore, to minimize legal and reputational risks for the organization, companies must refrain from imposing pressure or penalties on those who lawfully exercise their right to refuse testimony.

3 RELEVANT CASES

First fines imposed under the Digital Markets Act

On April 30, 2025, the European Commission imposed its first fines for non-compliance with the Digital Markets Act ("**DMA")**, which has been in force since March 2024. The fines, amounting to €500 million and €200 million, mark a decisive step toward the firm enforcement of this new regulatory framework.

The violations involved breaches of two key provision:

i. Article 5.4 of the DMA, which requires companies designated as gatekeepers to allow professional users, free of charge, to (a) communicate and promote offers to end users obtained through their core platform service or other channels, and (b) enter contracts directly with those end users.

ii. Article 5.2 of the DMA, which establishes obligations regarding the processing, combination and cross-referencing of personal data from users of online platforms.

These decisions demonstrate that the DMA is not merely a punitive mechanism but also a tool for fostering structured regulatory dialogue. However, they also underscore the significant risks of non-cooperation or partial compliance. Future decisions may impose even harsher penalties if infractions are repeated or become systemic.

Admissibility of evidence obtained through private investigators and workplace monitoring

The Supreme Court has upheld the use of evidence obtained by private investigators in an investigation concerning an employee's representative to verify the proper use of union leave, despite the company's lack of reasonable suspicion of misuse in the case analyzed.

According to ruling 2124/2025 of May 7, 2025, employer oversight of union leave is permissible, provided it does not constitute a singular, permanent and disproportionate monitoring that undermines the representative's independence or violates his or her fundamental rights.

This ruling is notable because, traditionally, caselaw has required well-founded suspicions, significant indications, or prior misconduct to justify highly intrusive control measures, such as surveillance through private investigators or hidden video surveillance. Also, employer oversight of employee representatives has typically been interpreted restrictively, given the enhanced protection granted to freedom of association.

4. Beyond our borders: International trends and developments

4 BEYOND OUR BORDERS: INTERNATIONAL TRENDS AND DEVELOPMENTS

U.S. | New DOJ Guidelines for Investigations and Enforcement of the Foreign Corrupt Practices Act (FCPA)

What has changed and how will it affect multinationals?

On June 9, 2025, the U.S. Department of Justice ("**DOJ**") released long-awaited new guidelines reactivating enforcement of the Foreign Corrupt Practices Act ("**FCPA**") following a 180-day moratorium initiated by an executive order on February 10, 2025.

From now on, the DOJ will explicitly prioritize cases with a clear connection to U.S. strategic interests, including:

- links to cartels or transnational criminal organizations;
- bribes involving critical infrastructure, defense or intelligence; and
- practices that may affect the competitiveness of U.S. companies in key markets.

The revised policy also decreases the likelihood of investigations into routine or low-value cases, focusing instead on conduct strongly indicative of intentional corruption. Therefore, so-called "facilitation payments" or minor bribes, if lawful under local laws, will largely be excluded from DOJ scrutiny.

While the DOJ guidelines are not specifically targeted at non-U.S. companies, any multinational operating in areas that affect U.S. interests should prepare for potential DOJ scrutiny.

RECOMMENDATIONS

The DOJ's updated FCPA strategy requires multinational companies, and particularly European companies with ties or interests in the U.S., to reassess their compliance policies and strengthen oversight of their global operations. Recommended actions include the following:

- **Risk mapping by geography and sector**: Identify operations, partners and projects exposed to strategic sectors or jurisdictions considered sensitive by the U.S.
- **Enhanced third-party diligence**: Intensify assessments and monitoring of suppliers, agents and business partners, particularly in complex supply chains.
- **Strengthen compliance programs**: Review and update compliance and anti-corruption programs to align with international standards while ensuring preparedness to address DOJ requirements.
- **Be prepared for audits and DOJ requests**: Establish internal protocols to efficiently manage and document audits, investigations and information requests from the DOJ.

4 BEYOND OUR BORDERS: INTERNATIONAL TRENDS AND DEVELOPMENTS

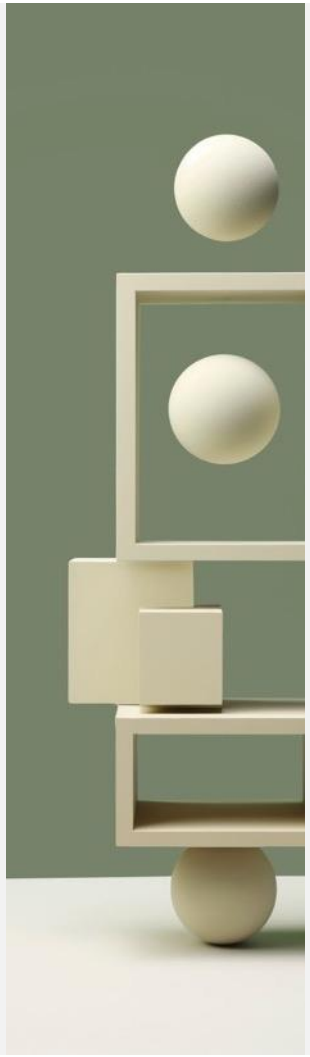
Peru | First conviction under the corporate administrative liability regime for criminal offense

In accordance with Act No. 30424, which governs the administrative liability of legal entities in criminal proceedings, and the Peruvian Criminal Code, legal entities can be independently investigated and sanctioned, regardless of the liability of the natural person perpetrating the offense. This applies to specific crimes such as corruption, money laundering, terrorism financing, tax and customs violations, parallel accounting, and crimes against cultural heritage committed by legal entities' directors, employees or representatives on their behalf or for their direct or indirect benefit.

However, article 17 of Act No. 30424 expressly provides that a legal entity may be exempt from liability if, before the crime was committed, it had effectively adopted and implemented a crime prevention model within its organization.

Mexico | Proposed amendments to the Federal Economic Competition Act

On April 25, 2025, the Federal Executive announced a significant proposal to amend the Federal Economic Competition Act. The proposal includes several key changes, such as (i) establishing a new regulatory body (the National Antitrust Commission); (ii) increasing fines for antitrust infringements; and (iii) streamlining procedures to expedite resolutions. See more.



Colombia | New anti-money laundering obligations for transportation companies

Colombia's Superintendence of Transportation ("**SuperTransporte**") has issued Resolution 2328 of 2025, replacing the previous Comprehensive Risk Management System for Money Laundering, Terrorism Financing, and Financing of the Proliferation of Weapons of Mass Destruction (SIPLAFT) with the new Risk Management System for Money Laundering, Terrorism Financing, and Financing the Proliferation of Weapons of Mass Destruction (SARLAFT).

This update introduces new compliance obligations that must be implemented by all companies under supervision, regulation or inspection of SuperTransporte by November 6, 2025.

This modification is particularly important for Spanish companies with subsidiaries in Colombia operating in the transportation sector. If subject to SuperTransporte's oversight, they must adjust their internal procedures to comply with the new regulations.

5. Cuatrecasas events

5 CUATRECASAS EVENTS

PAST EVENTS

- The NIS2 Directive in Spain and its impact on cibersecurity

  BARCELONA AND MADRID | May 7 and June 10

  Summary of the sessions | Documentation

- ¿What we do expect in 2025? – The most important developments in Compliance

  BILBAO | May 15

  Summary of the sessions | Documentation

- Internal investigation: an essential tool for criminal prevention and defense

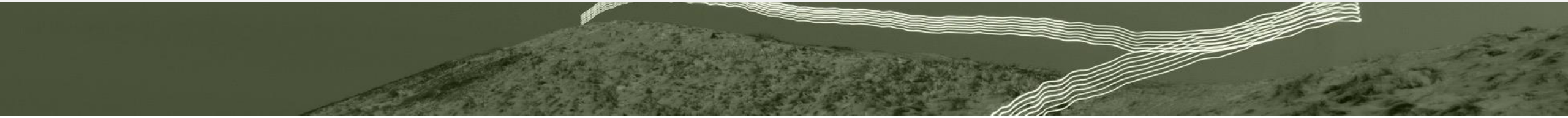
  MÁLAGA | June 10

  Documentation

- Present and future of the application of Competition Law

  BARCELONA | June 17

  Summary of the session



5 CUATRECASAS EVENTS

PAST EVENTS

- Data protection: What happened in the last year?

  ONLINE | June 18

  Documentation

- Responsible Artificial Intelligence for an Inclusive and Equitable Society

  MADRID | July 9

  Documentation

5 UPCOMING EVENTS

Annual Compliance & Investigations Day: 2nd edition returns

After the success of the first edition, which brought together more than 250 professionals, on **November 6, 2025** we will return with a new edition of this meeting that will be held simultaneously in **Madrid and Barcelona.**

We will have the participation of renowned experts who will address challenges in regulatory compliance, risk prevention and legal defense.

Don't forget to save the date in your calendar.

Add to calendar*

What topics would you like to cover?

We have prepared this space where you can send us your suggestions so that they can be evaluated for the meeting.

Your participation is key to making it even more relevant and enriching.

* Your registration is not confirmed for this event. You will be able to once it is published on our website.

THE EDITORIAL TEAM

Diego Pol

Partner Head of Compliance & Investigations

Marta Puertas

Compliance & Investigations Associate

Ramon Baradat

Intellectual and Industrial Property Associate

Danae Travé

Labor Associate

Pablo Garcia

Competition & Foreign Investment Associate

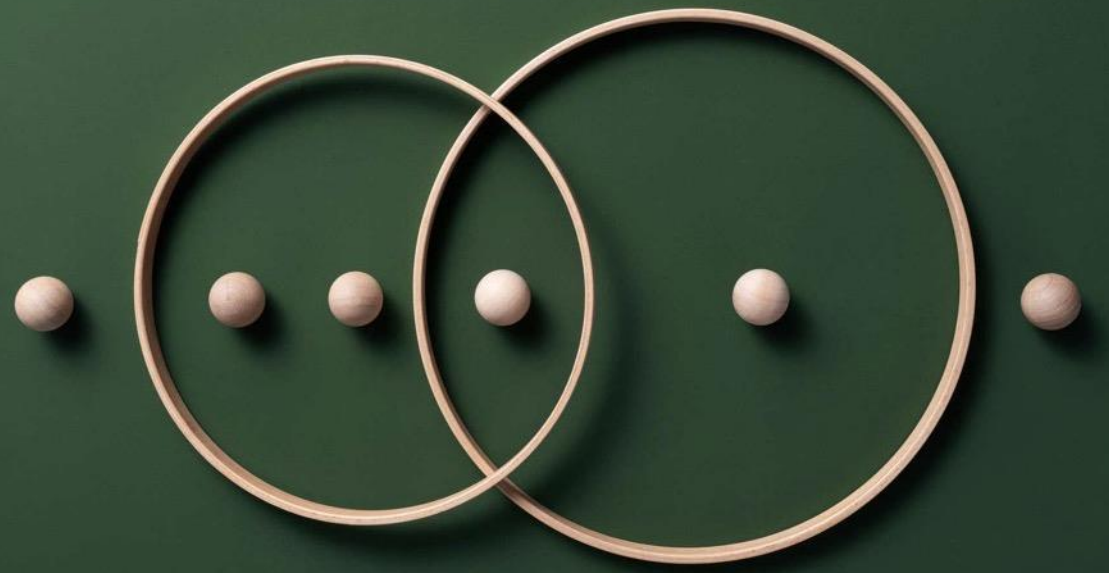
Patricia Boada

Senior Knowledge lawyer ACI

COMPLIANCE &
INVESTIGATIONS

CUATRECASAS COMPLIANCE CORNER

2ND EDITION. JULY 2025



CUATRECASAS