Internal Information System Policy

and

Information Management Procedure

CIMD Group

September 2026

VERSION HISTORY

Version	Date of Preparation	Author	Description of Changes
1.0	November 2023	Supervisory and Control Body for the Prevention of Crime	Original version approved by the CIMD Group's Governing Bodies
2.0	May 2024	Supervisory and Control Body for the Prevention of Crime	Incorporation of Intermoney Capital, S.G.E.I.C, S.A.
3.0	November 2025	Supervisory and Control Body for the Prevention of Crime	Adjustment of the scope of application
4.0	September 2026	Supervisory and Control Body for the Prevention of Crime	Update on the members of the Supervisory and Monitoring Body

Contents

1. Introduction

This document sets out the policy necessary to ensure that the Internal Reporting System and the information management procedure comply with the requirements laid down in Law 2/2023 of 20 February, regulating the protection of persons reporting regulatory infringements and combating corruption (hereinafter, Law 2/2023), which transposes into Spanish law Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

The purpose of this **Policy on the Internal Reporting System and Information Management Procedures** is to set out the principles governing the internal reporting system and the provisions established for the proper handling of information received within the framework of that system, and thereby to provide adequate protection against any reprisals that may be suffered by individuals who, in a work or professional context, report any of the acts or omissions listed in Article 2 of Law 2/2023.

2. Scope of application

Corretaje e Información Monetaria y de Divisas, S.A. (hereinafter "CIMD, S.A.") is the parent company of the CIMD Group, an independent financial group specialising in brokerage, consultancy, securitisation and management in the securities and energy markets of southern Europe.

This Policy applies to all subsidiaries of CIMD, SA established in Spain and, where applicable, to their own subsidiaries, which, at any given time, form part of the CIMD Group.

This Policy is approved by the Board of Directors of the parent company CIMD, SA, as well as by the governing bodies of the Spanish companies forming part of the CIMD Group, and applies to all their directors and employees regardless of their position, responsibility or hierarchical level, covering any area or department and any territorial or geographical scope in which they carry out their duties. Those in positions of responsibility must ensure that the staff under their supervision are aware of and comply with this Policy.

The application of this document to subsidiaries outside Spain must be preceded by an analysis of its content in relation to the regulatory requirements of the relevant jurisdiction, with such application being subject to the local regulations of the country in which the subsidiary is incorporated.

The Internal Reporting System comprises various communication channels through which the following matters may be reported:

- Acts or omissions that may constitute serious or very serious criminal or administrative offences.

- Acts or omissions that may constitute breaches of European Union law, taking into account the provisions set out in Law 2/2023.

- Breaches of labour law relating to health and safety at work which may constitute serious or very serious criminal or administrative offences.

Notwithstanding the possibility of receiving other reports relating to other areas of legislation, only those communications set out in Article 2 of Law 2/2023 shall be covered by the protective measures established therein.

However, Article 10(b) of Law 2/2023 stipulates that legal persons falling within the scope of application regarding the prevention of money laundering or the financing of terrorism are obliged to have an Internal Reporting System in place. Consequently, reports and/or communications submitted by a whistleblower on this matter will fall under the Internal Reporting System.

The persons with access to the CIMD Group's Internal Reporting System and subject to the protective measures under Act 2/2023 are:

- Employees and members of the governing bodies of the companies within the CIMD Group.
- Interns and trainees.
- Agents.
- Contractors, suppliers and any person working for or under the supervision and direction of such contractors and suppliers.
- Shareholders.
- Former employees.
- Job applicants.

3. Principles and safeguards of the Internal Reporting System

Compliance with applicable laws and internal regulations is the responsibility of all members of the CIMD Group. In this regard, there is a duty to report any incident that may constitute a criminal offence or irregularity.

Principle of Legality

The Internal Reporting System is founded on the principle of legality, incorporating and reflecting the principles and provisions of Law 2/2023.

Specifically, the Internal Reporting System shall be governed by the right to information, the right of defence, the right to the presumption of innocence of the person against whom a complaint is made, and the right to honour of all persons against whom a complaint is made and/or who are affected. The accused has the right to be informed of the acts or omissions attributed to them by means of a concise statement of the facts and to be heard at any time, in whatever manner is deemed appropriate to ensure the successful conclusion of the investigation.

Confidentiality and anonymity

The Internal Reporting System shall guarantee the confidentiality of the identity of the whistleblower and of any third party mentioned in the reports, of the information provided, and of the procedures carried out in the handling and processing thereof. The system in place ensures

that those involved in the processing and investigation of reports act with the utmost discretion regarding the facts of which they become aware by virtue of their position or role.

Access to the information is restricted to those with management authority as defined in this document, and the disclosure of any information regarding the reports is expressly prohibited.

Reports submitted to the Internal Reporting System may be either named (identifying the whistleblower) or anonymous.

In the event that a report is submitted anonymously, the tracing and tracking of such reports is prohibited.

No reprisals: protection of the whistleblower

The absence of retaliation and the protection of the whistleblower or other persons involved or associated with them – provided that reports are made in good faith and in accordance with the regulations, and that the whistleblower's protection is ensured – is an essential element of this Policy. Acts constituting retaliation, including threats of retaliation and attempts at retaliation against persons who make a report, are expressly prohibited.

Retaliation is understood to mean any acts or omissions that are prohibited by law or that, directly or indirectly, constitute unfavourable treatment which places those who suffer them at a particular disadvantage compared to others in the workplace or professional context, solely because of their status as whistleblowers or because they have made a public disclosure.

For the purposes of Law 2/2023, the following, amongst others, are considered to constitute retaliation: suspension of the employment contract, dismissal or termination of the employment relationship, demotion or refusal of promotion, intimidation, harassment, discrimination, or unfavourable or unfair treatment.

Whistleblowers shall not be held liable in respect of access to information that is communicated or disclosed publicly, provided that such access does not constitute a criminal offence. Whistleblowers reporting the infringements set out in paragraph 2 shall be entitled to the support measures laid down in Article 37 of Law 2/2023.

Independence and impartiality

All actions shall be carried out at all times with independence and impartiality and with the utmost respect for legislation and internal regulations. Complaints shall always be handled fairly, thoroughly, objectively, independently and honestly.

Transparency and accessibility

Information relating to the Internal Reporting System is provided in a clear and easily accessible manner, with sufficient publicity regarding its use and the guiding principles and safeguards, at in a separate and easily identifiable section on the CIMD Group's corporate website. The information provided must meet criteria of truthfulness and good faith, avoiding the provision of information that is confusing, false or lacking in accuracy. Any breach of the provisions of this Policy may result in disciplinary measures being imposed.

Traceability and security

Reports submitted via the Internal Reporting System, and subject to the provisions of this Policy, shall be recorded and processed in accordance with the regulations, whilst preserving the integrity of the information provided. When processing complaint files, the right of all persons involved to have their personal data and private information processed in accordance with the applicable personal data legislation in each case shall be respected.

Good faith

In accordance with the provisions of Law 2/2023, reports must always be submitted via the Internal Reporting System in good faith.

Reports shall be deemed to have been submitted in bad faith where the identity of the whistleblower has been misrepresented, or where they relate to facts known to be untrue, or involve persons who have had no connection with such facts, even if the facts themselves are true.

4. Reporting Channels

The various types of reporting channels are listed below:

1. Internal channels:

The Whistleblowing Channel is the preferred means of reporting the acts or omissions covered by Law 2/2023, which effectively safeguards against breaches of the Internal Information System Policy and the Information Management Procedure, whilst preventing any risk of retaliation against the person making the report.

This channel allows written reports to be submitted via the following methods; reports may be submitted either anonymously or with the informant's identity disclosed:

- The online platform, located on the CIMD Group's website, accessible at the following address: https://www.grupocimd.com/canal-de-denuncias/
- Email: organovigilanciaycontrol@grupocimd.com
- Postal address: Surveillance and Control Body, Príncipe de Vergara 131, 3rd Floor, 28002 Madrid.

Whistleblowers may also make a report verbally, requesting that the Supervisory and Control Body send the report by email, attaching a voice message file.

The whistleblower may also request a face-to-face meeting by writing to the channels indicated above; this meeting will take place within seven days of the request. Such a meeting shall be documented in one of the following ways, subject to the whistleblower's consent: (i) by recording the conversation in a secure, durable and accessible format; or (ii) by means of a complete and accurate transcript of the conversation drawn up by the staff responsible for processing it. Without prejudice to the rights to which they are entitled under data protection

legislation, the whistleblower will be given the opportunity to check, correct and sign to confirm the transcript of the conversation.

2. Other channels:

As the companies forming the CIMD Group have other communication channels, including the email address: consultasprevencionacoso@grupocimd.com, which facilitate the submission of reports, complaints and/or claims relating to other regulatory areas, only those communications set out in Article 2 of Law 2/2023 shall be covered by the protective measures established therein.

Should a whistleblower report an irregularity via channels other than the Whistleblowing Channel and the recipient of such a report identify that the report falls within the scope of the Internal Reporting System, the recipient must inform the whistleblower of the existence of the Whistleblowing Channel so that the report can be submitted via that channel.

3. External reporting channel – Independent Whistleblower Protection Authority (A.A.I.):

Irrespective of the establishment of internal reporting channels, any individual may report to the Independent Whistleblower Protection Authority (A.A.I.), or to the relevant regional authorities or bodies, any acts or omissions falling within the scope of Law 2/2023, either directly or following a prior report made via the Whistleblowing Channel.

5. Information Management Procedure

Receipt and Registration

Any person identified in section 2 of this document who has access to the CIMD Group's Internal Reporting System may submit a report via any of the internal channels identified above.

The whistleblower must provide the information deemed necessary.

In the case of reports submitted by means other than the online platform, email, post or in-person meeting – whether these are reports made by the whistleblower themselves or those forwarded to the System Manager by a person who has received the report but is not responsible for handling it – they will be incorporated into the Whistleblowing Channel once the information and documentation provided by the whistleblower has been obtained.

Within a maximum of seven calendar days, the Head of the Internal Reporting System must send an acknowledgement of receipt of the report to the whistleblower, unless this would jeopardise the confidentiality of the report.

As part of the handling of the report, whether before and/or after it has been accepted, it may be necessary to contact the whistleblower to request further information, clarify certain aspects or even provide support. The method used to maintain contact depends on the requirements of the case and the internal channel through which the report was received; it is recommended that communications be supported by documentary evidence.

Particularly during the course of the investigation, but also prior to it, it may be necessary to implement certain protective measures, such as ensuring that those involved do not share the

same workplace or managing conflicts of interest should any of the individuals involved in a report be related by blood, marriage or affinity to any of those involved in its handling, investigation or resolution.

Analysis of the complaint: admissibility or inadmissibility

Reports submitted will be subject to an admissibility assessment, and reports that fall outside the scope of the Internal Reporting System are excluded where:

- Do not fall within the material scope of Law 2/2023.
- Are submitted by a group without access to the Internal Reporting System.
- Have been rejected by any internal reporting channel.
- Relate to facts available to the public (public information).
- Relate to complaints concerning interpersonal conflicts or which affect only the whistleblower and the persons to whom the communication or disclosure refers.
- Are based on mere rumours and/or are not grounded in specific or concrete suspicions or evidence.
- They relate specifically to the content of a file or document not accessible to the CIMD Group companies identified in the complaint and not provided in the report.
- Relate to events or conduct that are already under investigation by the police, administrative inspection bodies and/or the courts.

However, the Head of the Internal Reporting System reserves the right to accept a report which, despite not meeting the admissibility criteria, involves an exceptional circumstance requiring handling through the Internal Reporting System.

The admissibility assessment shall be carried out by the Head of the Internal Reporting System, who must inform the whistleblower of the outcome of that assessment. The Head of the Internal Reporting System may consult external experts in order to reinforce the independence, objectivity and respect for the safeguards offered by the Internal Reporting System.

Investigation of the complaint

The investigation will be carried out in accordance with the procedures, principles and safeguards set out in this Policy and, in all cases, whilst safeguarding the rights of the individuals concerned.

The investigation procedure may include any investigation or evidence deemed relevant and useful, subject to the principle of proportionality so that it is as least burdensome as possible in relation to the legal position of the person concerned.

A register is kept of the information received, which will record all the steps taken and any internal investigations that have resulted from them, whilst ensuring the confidentiality of the information.

Conclusion

The investigation process shall be duly documented, setting out the background, the objective, the scope and the conclusions reached.

The maximum timeframe for responding to the investigation proceedings shall not exceed three months from the date of receipt of the report, except in cases of particular complexity requiring an extension of the timeframe, in which case it may be extended by a further maximum of three months.

If, during the preliminary assessment or investigation phase, the facts reported appear to constitute a criminal offence, the information shall be forwarded immediately to the Public Prosecutor's Office; and where the facts affect the financial interests of the European Union, they shall be forwarded to the European Public Prosecutor's Office.

6. Protective measures

Persons who report or disclose infringements referred to in paragraph 2 shall be entitled to protection provided that the following circumstances apply:

- They have reasonable grounds to believe that the information in question is true at the time of the report or disclosure, even if they do not provide conclusive evidence, and that the said information falls within the scope of this Act.

- The reporting or disclosure has been made in accordance with the requirements set out in Act 2/2023.

Persons who have reported information on acts or omissions anonymously and who have subsequently been identified shall also enjoy the same protection.

Persons excluded under section 5, *'Examination of the complaint: admissibility or* inadmissibility', are expressly excluded from this protection.

7. Protection of personal data

All actions carried out within the framework of this Policy shall be conducted in compliance with current data protection regulations.

The Internal Reporting System is designed, established and managed securely, so as to guarantee the confidentiality of the individuals involved in the reports and of the procedures carried out in the management and processing thereof, as well as data protection.

The processing of personal data arising from the application of Law 2/2023 shall be governed by the provisions of Title VI thereof and by the applicable legislation in this area.

Whistleblowers will be informed that their identity will be kept confidential at all times and will not be disclosed to the persons to whom the reported facts relate or to third parties.

Access to the personal data contained in the Internal Reporting System shall be limited to those with management authority in accordance with their assigned duties; the disclosure of any information regarding the reports to unauthorised persons is expressly prohibited. In any event, access to this data shall be restricted, within the scope of their powers and duties, exclusively to:

- The System Manager and the person responsible for managing it.
- The Director of Human Resources, only where disciplinary measures may be taken against an employee.
- The Head of Legal Affairs, should legal action be required in relation to the facts set out in the report.
- The designated data processors.
- The Data Protection Officer.

The processing of data by other persons, or even its disclosure to third parties, shall be lawful where necessary for the adoption of corrective measures within one of the companies of the CIMD Group or for the handling of any disciplinary or criminal proceedings that may be applicable.

Personal data whose relevance to the processing of specific information is not apparent will not be collected; if such data is collected accidentally, it will be deleted without undue delay.

Personal data subject to processing will be retained in the Internal Information System only for as long as is strictly necessary to decide whether to initiate an investigation into the reported facts. If the report is rejected on the grounds that it does not meet the defined admissibility criteria, the data will be deleted, unless the rejection was due to the report being untrue and this could constitute a criminal offence, in which case the information will be retained for as long as necessary whilst the legal proceedings are ongoing.

In any event, three months after receipt of the report, if no investigative proceedings have been initiated, the personal data will be deleted, unless the purpose of retention is to provide evidence of the functioning of the Internal Reporting System. Reports that have not been acted upon may only be retained in anonymised form, and the obligation to block such data shall not apply.

Those with access to the Internal Reporting System, as set out in section 2 of this document, shall be informed about the processing of personal data.

8. Data Controller for the Internal Reporting System

The Governing Bodies of the CIMD Group companies have designated the Supervisory and Control Body of the Criminal Compliance Department as the sole Data Controller for the Internal Reporting System, and this body is responsible for its management.

The body as mentioned above is composed of Ms Beatriz Senís Gilmartín and Ms María Aguirre Rodríguez.

This Responsible Party, as a collegiate body, shall act autonomously and independently of any other bodies, committees or commissions of the CIMD Group entities.

9. Review and publication of the Internal Reporting System Policy and the Information Management Procedure

A programme is established for the review of the Internal Reporting System Policy and the Information Management Procedure with the aim of identifying potential areas for improvement, or in the event of possible changes to current regulations.

The Supervisory and Control Body shall be responsible for this review.

The Supervisory and Control Body shall also be responsible for ensuring the accessibility of this document by publishing it both on the CIMD Group's corporate website and on the Corporate Intranet in the 'Policies' section.