	Incident management and whistleblowing policy	Reference I.4 Version : 1.3

Liability	
Person responsible for the procedure	Pascale BRADBURY
Department	All employees
Relay correspondent	Pascale BRADBURY

Purpose of the procedure

In accordance with regulations, LONVIA CAPITAL has set up a procedure and a tool enabling all its employees and external individuals to:

- Report breaches of the law using an alert processing tool to guarantee the anonymity of the whistleblower.
- Report any failure or compliance breach to the person responsible for managing the alert system/the Compliance Officer.

Through the system described to centralise and process identified anomalies, LONVIA CAPITAL aims to:

- Identify and manage high-risk areas.
- Improve processes and procedures where necessary.
- Provide practical case studies for the annual assessment of certain service providers.

List of tools/applications used	
Tools	Excel; PDF
Application(s)	Outlook; integrityLog by Euronext

List of statements used	Archiving (yes/no)	Storage location
Incident form	Yes	
Incident base	Yes	

Managing procedure updates

Version	Date	Status	Author of changes	Nature of the changes
1.0	06/04/2020	Completed	AGAMA CONSEIL	Creation
1.1	10/09/2020	Completed	J-B BARENTON	Name modification and validation
1.2	23/11/2023	Completed	P BRADBURY	Incorporation of changes to whistleblower rights, addition of the IntegrityLog tool and Appendix for Spain
1.3	17/06/2024	Completed	P BRADBURY	Formatting

Contents

1. DEFINITIONS

An **incident** is an event that occurs and alters the expected and normal course of events. It materialises an operational risk.

The Basel Committee defines **operational risk as** "the risk of loss arising from inadequate or failed internal processes, people and systems or external events". Operational risk includes

- Incidents caused by human error, fraud or malicious intent.
- Failures in information systems.
- Problems related to personnel management.
- Commercial disputes, accidents, fires, floods.

Processing of personal data" means any operation or set of operations relating to personal data, regardless of the process used (collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment).

An incident is also considered to be an event that constitutes a serious reputational risk for LONVIA CAPITAL and is caused by the conduct of a client, employee or service provider.

However, client complaints do not fall within this scope. Regulations precisely define the conditions for handling client/holder complaints and LONVIA CAPITAL has set up a specific procedure for this purpose.

A breach indicates any employee's doubt as to whether an operation or activity actually complies with regulations or internal procedures.

Whistleblowing is a system available to employees, enabling them to report problems that could seriously affect a company's business or give rise to serious liability.

2. REPORTING AND HANDLING OF BREACHES AND INCIDENTS

A. Detecting and communicating failures/breaches or incidents

All LONVIA CAPITAL employees undertake to inform the Compliance Officer without delay of any incidents observed, whether or not they were involved in the event or whether the breach was caused by a service provider or the company itself.

The employee records this failure/breach on the "operational or IT incident report form"[1] provided for this purpose, filling in all the fields identifying the breach?? on which they have information.

The operational or IT incident report form is then sent to the CO along with all the available documentation needed to fully understand the breach. The CO conducts an initial analysis based on the nature and actual or potential impact of the reported incident.

It is advisable for the reporting employee to propose a corrective action, which is initiated after validation by the CO. They may also ask the CO for advice on the corrective action to be taken.

[1] Appendix 1

B. Management of the breach

Analysis of the alert by the CO enables a typology to be established. The incident may concern a one-off internal error, the failure of an information system, a mistake by a service provider, etc. The CO thus assesses the operational risk resulting from the breach attributable either to procedures, internal systems or external events.

If necessary, the CO takes measures to prevent the breach from recurring, such as reinforcing the system, stepping up first-level controls, modifying the corresponding operational procedure, etc.

The CO monitors and takes part in resolving the incident. The incident's resolution and closure are recorded on the incident form. Finally, the operational or IT incident report form is signed by the Compliance Officer.

The CO may also take steps to raise employee awareness, depending on the level of risk associated with the breach detected.

All documents and any exchanges relating to the handling of the breach are recorded in a dedicated file on the LONVIA CAPITAL server and filed in a physical file.

Any incident for which LONVIA CAPITAL has applied a disciplinary measure due to breaches of its professional obligations, with regard to an individual holding the CO card, must be notified to the Autorité des Marchés Financiers within a maximum period of one month by the manager of the company.

C. Updating the incident database

The CO fills in the "Incident database"[2] . The CO or their delegate uses this database periodically to monitor the frequency of incidents, the time taken to rectify them, the corrective measure implemented and plans to improve the procedures in place.

This "Incident database" is also used to support the annual assessment of service providers carried out by LONVIA CAPITAL.

D. Responsibilities of management and supervisory bodies

The AMF's General Regulation has introduced a rule for asset management companies managing UCIs, which requires LONVIA CAPITAL's executive directors to report to the AMF without delay:

- Incidents likely to result in:
  - A loss or a gain.
  - A cost related to civil or criminal liability.
  - A cost related to an administrative penalty.
  - Damage to reputation.

  And for which the impact exceeds 5% of Regulatory Capital

- Any event no longer enabling LONVIA CAPITAL to meet the conditions of its authorisation.

[2] Appendix 2

This declaration takes the form of an incident report disclosing the nature of the incident, the measures adopted and the initiatives taken to prevent its recurrence.

3. WHISTLEBLOWING

Law no. 2022-401 of 21 March 2022, aimed at improving the protection of whistleblowers, provides a broader definition of whistleblower, simplifies reporting channels, extends protection against retaliation against the whistleblower's family and friends.

The decree of 3 October 2022 sets out the procedures for establishing internal and external procedures for collecting and processing whistleblowing alerts.

In accordance with the provisions of Law 2/2023 of 20 February regulating the protection of whistleblowers who report breaches of regulations and the fight against corruption, LONVIA CAPITAL, SUCURSAL EN ESPAÑA ("LONVIA branch") has set up an internal whistleblowing system. (Appendix 4)

A. Internal system

Any employee may use IntegrityLog at the following address Whistleblower (complylog.com), to report information without direct financial compensation and in good faith on:

1. a crime or wrongdoing.
2. a threat or harm to the general interest.
3. a breach or an attempt to conceal a breach of:
    - ✓ an international commitment duly ratified or approved by France.
    - ✓ a unilateral act by an international organisation taken on the basis of such an undertaking.
    - ✓ European Union law.
    - ✓ the law or regulations.

In a professional context, whistleblowers can now report events that have simply been brought to their attention.

The scope of ethical or professional whistleblowing is set out in the CNIL guidelines on professional alert systems. (Appendix 3)

The whistleblower is free to choose the channel, internal or external, by which they communicate.
In the case of LONVIA's internal channel, information can be submitted via the Whistleblower channel (complylog.com), which guarantees the anonymity of the whistleblower, or, in person, by e-mail, using the form.

Whistleblowers are protected and will not be subject to discriminatory measures, particularly in terms of dismissal, remuneration or training. By warning the person responsible for handling alerts (LONVIA's Compliance Officer), the whistleblower is not exempt from liability if they have breached the rules themselves.

The confidentiality of whistleblower data is guaranteed throughout the process of managing the information transmitted.
In this respect, access to personal data contained in the whistleblowing policy is limited exclusively to the following persons, within the scope of their powers and duties:
(A) The person responsible for the system and any person who directly manages the system.
(B) The Director of Human Resources, only when disciplinary measures may be taken against an employee.
(C) The person responsible for LONVIA's legal services, if it proves necessary to take legal action in relation to the facts described in the communication.
(D) People responsible for data processing who may be appointed from time to time.
(E) The data protection officer.

Whistleblowers have the right to know the status of their communication and its outcome within the deadlines set by law 2/2023.

Law 2/2023 establishes that the processing of personal data arising from its application will be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, GDPR); in the organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights; and in Title VI of Law 2/2023 itself.
The Head of the Internal Information System is responsible for processing the data received via the established internal information channel.

LONVIA CAPITAL's CO records the information on a durable medium that can be consulted by the AMF. Since 1 September 2022, whistleblowers have been able to choose freely between two reporting channels: internal and external, with no hierarchy between them.

B. Notifying the AMF

The whistleblower may therefore apply the external procedure without first using the internal whistleblowing procedure. Similarly, direct public disclosure is permitted in certain cases.
In addition, the AMF has set up a system for receiving and handling alerts about potential breaches of the regulations it oversees, which guarantees the confidentiality of the whistleblower and the persons concerned, pursuant to Act 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life.

The AMF undertakes to treat as confidential any alerts it receives through procedures set up within the AMF.

To report any event that a LONVIA CAPITAL employee knows is in breach of European legislation, the Monetary and Financial Code or the AMF General Regulation, the employee may contact the AMF:

- https://www.amf-france.org/fr/lanceur-dalerte
- By post at:

AMF Legal Affairs Department/Direction des affaires juridiques
17 place de la Bourse
75082 Paris Cedex 02
by marking the envelope "CONFIDENTIEL" (or by following the procedure described above in special cases)

- By telephone: +33 (1) 53 45 64 44 from 9am to 12pm and from 2pm to 5pm

For reasons of confidentiality, it is recommended that the employee's personal e-mail service or personal telephone be used rather than those of LONVIA CAPITAL. The AMF undertakes to ensure that only specialised AMF staff will handle the case and have access to the identity of the whistleblower and the designated perpetrator, and to provide appropriate and careful follow-up of the case brought to their attention. The AMF undertakes to ensure that the whistleblower's case is followed up regularly by specialised staff only.

C. Feedback sent directly to the Défenseur des droits (human rights defender)

Note that if the employee has doubts about which body is competent to receive and deal with the alert, it may be sent to the Défenseur des droits, who will direct the employee to the appropriate body.

Urgency justifying non-referral of the matter to the body in question if the events in question appear to constitute:

- Serious and imminent danger.
- Or a risk of irreversible damage.

The employee may report the matter directly to:

- The judicial authority.
- The administrative authority.
- The professional body.

These establishments may be contacted alternatively or simultaneously. It is preferable to make the referral by recorded delivery with acknowledgement of receipt.

It is also recommended that the following transmission procedures be followed to ensure compliance with confidentiality rules:

- The report must be sent by post, in writing and in a double envelope.
- All the elements of the report must be inserted in a closed envelope - known as the inner envelope - which will be inserted inside a second envelope addressed to the Human Rights Defender, known as the outer envelope.
- The inner envelope must bear only the following wording: "SIGNALEMENT D'UNE ALERTE (date of dispatch)" The outer envelope must bear the dispatch address:

Défenseur des droits Libre réponse
71120 75342 PARIS CEDEX 07
Défenseur des Droits (defenseurdesdroits.fr)

An acknowledgement of receipt will be sent to the employee with an identification number which they must use for all their dealings with the Human Rights Defender.

If the employee considers the alert to be particularly serious, they may also choose to make the alert public.

This exceptional mechanism should only be used with great discretion, as the whistleblower can only be held criminally irresponsible if their assessment of the urgency of the situation is indisputable. Public disclosure should therefore only be considered as a last resort if it is clearly impossible to act in any other way to put an end to the risk at the source of the alert.

APPENDIX 1: OPERATIONAL OR IT INCIDENT REPORT FORM

FICHE DE DECLARATION D'INCIDENT OPERATIONNEL OU IT

ZONE RESERVEE AU RCCI

Date réception | Date de clôture | Référence

Commentaire

EXPEDITEUR

Nom, Prénom | Département

IDENTIFICATION DE L'INCIDENT

Date incident | Date détection | PTF concernés

IMPACT FINANCIER

Gain/Perte/Nul | Montant | Devise

Incidence équivalent à %* des Fonds Propres Réglementaires

DESCRIPTION ET TRAITEMENT DE L'INCIDENT

Circonstances

Responsabilités

Mesure(s) de régularisation

Mesure(s) corrective(s) de prévention

**les incidents dont la survenance est susceptible d'entrainer : une perte ou un gain, un coût lié à la mise en cause de sa responsabilité civile ou pénale, un coût lié à une sanction administrative, une atteinte à la réputation, et dont l'incidence excède 5% des Fonds Propres Réglementaires doivent être déclarés à l'AMF sans délai.*

APPENDIX 2: INCIDENT DATABASE

Available in the procedures directory.

APPENDIX 3: PROFESSIONAL ALERT SYSTEM (PAS) GUIDELINES

Updating the reference framework for whistleblowing systems - CNIL

APPENDIX 4: WHISTLEBLOWING SYSTEM IN SPAIN

a. Introduction and background

The LONVIA CAPITAL (**"LONVIA**") Whistleblowing Policy contains the basic principles for management of incidents or breaches that may give rise to operational risks for LONVIA, as defined in the European Whistleblowing Directive, and also defines the whistleblowing procedure, also referred to as "ethical alert" or "whistleblowing" in the European Whistleblowing Directive.

This Appendix ("**Spanish WB Appendix**" or the "**Appendix"**) contains the specific features applicable to of LONVIA CAPITAL, SUCURSAL EN ESPAÑA ("**LONVIA Branch**"), in accordance with Law 2/2023 of 20 February, regulating the protection of persons who report regulatory breaches and the fight against corruption (**"Law 2/2023"**) and transposing Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 ("**WB Directive")** in Spain.

The implementation in Spain of the "**Whistleblowing Policy",** which consists of the **LONVIA Capital Whistleblowing Policy (for the Paris office)** and the **Spanish Whistleblowing Appendix**, was approved by the LONVIA Capital Board of Directors, without prior consultation with employee representatives, as there is no such body in Spain.

For all matters not covered in this Appendix, including the procedure to be followed in the event of receipt of information, LONVIA CAPITAL's whistleblowing policy shall apply.

b. LONVIA internal and external information channels

The LONVIA branch's internal information channel is Whistleblower (complylog.com). It is the preferred channel for reporting actions or omissions referred to in article 2 of law 2/2023, as indicated in section 4 of this document, which can be consulted via the following link:

Whistleblower (complylog.com)

Through the COMPLYLOG tool, the persons listed in this appendix may report any breach of the law, internal policies or LONVIA's Code of Conduct, as set out in this Whistleblowing Policy.

Similarly, the whistleblower (as defined in this policy) may request a meeting with the head of the LONVIA agency's internal system, with the meeting to take place within seven days of the whistleblower's request. The meeting will be recorded and a new procedure will be initiated at the start of the meeting.

In addition, people protected by the whistleblowing policy can contact the external channel set up by the independent whistleblower protection authority (to be created) or equivalent authorities at regional level (for reporting breaches relating to regional legislation).

To obtain information on any offences committed by the public administrations of Spain's autonomous communities and cities:

- Canal del Informante de la Comunidad de Madrid
- Anti-Fraud Office of Catalonia
- Valencian Anti-Fraud Agency
- Andalusian Anti-Fraud Office
- Office for Preventing and Combating Corruption of the Balearic Islands

For the notification of possible breaches in the field of securities markets: CNMV - Notification of possible breaches in the field of securities markets.

To report any breaches relating to money laundering and the fight against terrorism: SEPBLAC, the Spanish financial intelligence unit within the Bank of Spain.

In addition, as part of its whistleblowing policy, LONVIA has made available to all members of its organisation other information channels defined in this policy. In this case, the whistleblower will be subject to the procedures described in this policy[3].

c. Responsible for handling internal alerts

In accordance with the provisions of law 2/2023, a natural person has been appointed as the person responsible for the internal information system and carries out their duties autonomously and independently.

LONVIA's Board of Directors is responsible for appointing the LONVIA branch's Head of the Internal Information System and for notifying the Independent Whistleblower Protection Authority (a body currently being set up). LONVIA's Board of Directors has currently appointed a Head of the Internal Information System:

PASCALE BRADBURY
9 avenue de l'Opéra, 75001 Paris

[3] Referral to the MFA and direct referral to the Human Rights Defender

d. Scope of the whistleblowing policy

The whistleblowing policy and the protection it offers apply to people who report the following breaches:

Any act or omission that may constitute a breach of European Union legislation at any time, in accordance with Article 2 of Law 2/2023.

> *fall in the application scope of European Union acts listed in the Appendix to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law, irrespective of their qualification under national law.*
>
> *affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); or*
>
> *have an impact on the internal market, as referred to in Article 26(2) TFEU, including breaches of EU competition rules and State aid, as well as internal market breaches concerning acts contrary to the rules on corporation tax or practices aimed at obtaining a tax advantage which would defeat the object or purpose of the legislation applicable to corporation tax.*

Actions or omissions that may constitute a serious or very serious criminal or administrative offence. In any event, this includes all serious or very serious criminal or administrative offences that result in financial loss for the Treasury and social security.

This is without prejudice to certain limitations provided for by law 2/2023 (see article 2).

It also applies to people file cases on the subjects listed in LONVIA CAPITAL's whistleblowing policy.

e. Scope of the whistleblowing policy

The whistleblowing policy applies to the following people, known as whistleblowers:

Employees of the LONVIA branch in Spain and of LONVIA in France, in the latter case for questions concerning the LONVIA branch.

Self-employed workers who provide services to the LONVIA branch.

LONVIA shareholders and board members, for questions concerning the LONVIA branch.

Any person working for contractors, subcontractors or suppliers of the LONVIA branch or under their supervision and management.

Persons who have been employed by the LONVIA branch, volunteers, interns, interns in training and persons whose employment relationship has not yet begun in cases where information on breaches has been obtained during the selection procedure or pre-contractual negotiation.

People who assist the whistleblower in the reporting process and who may be subject to retaliation.

People linked to the whistleblower and likely to suffer retaliation, such as work colleagues or relatives of the whistleblower.

Legal entities for which the whistleblower works, or with which they have any other type of employment relationship or in which they have a significant shareholding.

f. Whistleblowers' rights

The whistleblower is free to choose the channel, internal or external, by which they communicate.

In the case of the LONVIA branch's internal channel, information may be submitted via the Whistleblower (complylog.com) channel, which guarantees the anonymity of the whistleblower, or in person, by e-mail, by writing to the person responsible for the whistleblowing system named above.

The confidentiality of whistleblower data is guaranteed throughout the information management process.

In this respect, access to personal data contained in the whistleblowing policy is limited exclusively to the following persons within the scope of their powers and duties:

The person responsible for the system and any person who manages it directly.

The Director of Human Resources, only when disciplinary measures may be taken against an employee.

The person in charge of LONVIA's legal department, should it be necessary to take legal action in relation to the facts described in the communication.

Data controllers who may be appointed from time to time.

The Data Protection Officer.

The whistleblower has the right to know how their case is progressing and its outcome within the time limits set by law 2/2023.

g. Data protection

Law 2/2023 establishes that the processing of personal data arising from its application will be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, GDPR); in the organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights; and in Title VI of Law 2/2023 itself.

The Head of the Internal Information System is responsible for processing the data received via the established internal information channel.

h. People concerned

In accordance with Law 2/2023, during processing of the report, the persons concerned by the communication are entitled to the presumption of innocence, to the right of defence and to the right of access to the report provided for by the aforementioned law, as well as to the same protection as that established for whistleblowers, preserving their identity and guaranteeing the confidentiality of the events and data of the proceedings.

i. False communications

Article 63 of Law 2/2023 states that it is a very serious offence to communicate or publicly disclose information in the knowledge that it is false.

j. Information management: Procedure

How to report

As indicated in the LONVIA CAPITAL whistleblowing policy, events falling within its scope may be reported through the channels indicated in the policy, while for events occurring within the scope of the LONVIA branch, in accordance with Law 2/2023, the Whistleblower (complylog.com) channel has been made available to the LONVIA branch.

In addition, any person who becomes aware of a complaint or information made outside the Whistleblower (complylog.com) channel must immediately inform the head of the LONVIA branch's internal information system, via the internal Whistleblower (complylog.com) channel, maintaining the utmost confidentiality regarding the

information received. Failure to comply with this confidentiality obligation may have serious consequences for the whistleblower and for LONVIA and will be subject to disciplinary proceedings for very serious misconduct.

The characteristics of the internal information channel and the principles governing its operation are as follows:

- Ensuring the confidentiality of the whistleblower's identity in internal communications and throughout the information management process.
- Provide for the possibility of maintaining communication with the whistleblower and, if deemed necessary, requesting additional information.
- Possibility of submitting anonymous proposals.
- Establishment of the right of the person concerned to be informed of the acts or omissions attributed to them and to be heard at any time.
- Demand respect for the presumption of innocence and the honour of those involved.
- Compliance with the provisions relating to the protection of personal data in accordance with the provisions of Law 2/2023.
- Immediate transmission of information to the public prosecutor when the events may reveal a criminal offence.

1. Information management

- **Receipt of information and preliminary assessment**

The information is received by the Head of the Internal Information System. (hereinafter, if applicable, the "**Recipient**").

The recipient acknowledges reception of the report to the sender within seven days.

For a report received digitally, this acknowledgement is automatic and takes the form of a registration number/password which is used by the whistleblower to follow the corresponding procedure and, if necessary, to receive communications from the recipient or to provide new information.

The beneficiary reports to the CO and, for information, to the Global Compliance Officer.

The CO, with the support of the head of the internal information system, will be responsible for sorting all the information received.

In this respect, the report will be subject to a preliminary review to verify its:

- integrity.
- compliance with the criteria and requirements set out in the whistleblowing policy.
- the existence of legal and/or factual conditions for launching the subsequent analysis phase.
- the potential seriousness of the alleged events and the urgency.

Once due diligence has been carried out:

- if the information received does not fall within the scope of the whistleblowing policy or does not comply with the requirements set out in the whistleblowing policy, the recipient or the person responsible for due diligence will classify it by informing the whistleblower (via the Whistleblower (complylog.com) channel).The reasons for not continuing with the analysis must be well documented and justified.
- if the information is too general or incomplete, the recipient or the person responsible for due diligence contacts the whistleblower via the referral channels to request additional information useful for the preliminary assessment.
- if the receiver or the person in charge of due diligence considers that the information falls within the scope, they move on to the subsequent analysis phase by informing the recipient.

This phase must be completed within 10 working days of receiving the information (this period may be extended to 15 working days if preliminary investigations are necessary).

At the end of the preliminary phase, the CO, in collaboration with the Head of the Internal Information System and using the internal or external resources deemed necessary, draws up a report (the "**preliminary report**") indicating the type of information, the date of receipt, the date of completion of the preliminary assessment and the result of the preliminary assessment (archiving or further analysis), as well as the reasons for the preliminary assessment.

2. Report analysis

If, following the preliminary audit, an investigation is necessary, the CO may delegate the performance of the investigation to human resources, local compliance, the systems security team or a third party specialising in the matter, and carry out, with the Head of the Internal Information System, supervision of the investigation (unless the events concern the Head of the Internal Information System, in which case they will not participate in the investigation).

At this stage, taking care not to reveal the identity of the whistleblower, the subjects concerned by the information and the purpose of the information, the person in charge of the analysis and assessment phase may (i) interact with other functions and areas of the company to request their collaboration, providing data, documents or information useful to the analysis itself; (ii) request additional elements or perceptions from the whistleblower, recording the corresponding interview; or (iii) request the opinion of third parties specialising in the specific subject on which the information is based.

The person responsible for the analysis and assessment phase shall carry out any activity deemed useful or necessary, including interviewing the whistleblower and/or any other person likely to provide information on the events reported, in compliance with the principles of confidentiality and impartial judgement, legislation on the protection of personal data and the relevant applicable employment contracts.

The person concerned by the information has the right to be informed of the acts or omissions of which they are accused and to be heard at any time. This communication shall take place at the time and in the manner deemed appropriate to ensure the smooth running of the investigation.

This entire process is carried out under the supervision of the Head of the Internal Information System.

3. Analysis results and final report

At the end of the analysis phase, the CO, in collaboration with the Head of the Internal Information System, whether or not they have delegated the execution of the investigation to another department or area of the entity or to a third party specialised in the field, draws up a final report ("**final report"**), which presents the following elements:

- details of the information (name of the whistleblower if the whistleblower consents, and of the person(s) reported, place and date of the events, evidence or documentation).
- the checks carried out, their results and the company or third parties involved in the analysis phase.
- a summary evaluation of the analysis process, with an indication of the cases found and the reasons for them.
- the result and conclusion of the analysis (archiving or justification of the report).

The final report will be sent to the LONVIA branch management body by the Head of the Internal Information System and will also be brought to the attention of the competent LONVIA body by the CO.

4. Decision-making measures

The maximum time limit for replying to the request for information may not exceed three months from receipt of the information, except in cases of particular complexity requiring an extension of the time limit, in which case the time limit may be extended by a maximum of three additional months.

On receipt of the final report, the Chief Executive Officer, with the advice of the Head of the Internal Information System, the Compliance Officer and the person in charge of the internal investigation, decides whether to initiate disciplinary proceedings against the person responsible for the offence or unlawful behaviour and held liable as a result of the analysis carried out and the assessment made.

The Head of the Internal Information System must inform the public prosecutor's office if these events are considered to be of a criminal nature or forward the information to another authority or body that may be competent to deal with the communication.

If the events affect the financial interests of the European Union, the information is passed on to the European Public Prosecutor.

5. Ban on retaliation

Acts constituting retaliation, including threats of retaliation and attempted retaliation against persons who submit a report or information through the Whistleblower (complylog.com) channel or by any other internal means, or to the Independent Whistleblower Protection Authority or equivalent authorities of the Autonomous Communities, or who make a public disclosure in accordance with the criteria and requirements of Law 2/2023, are strictly prohibited.

For the purposes of the whistleblowing policy, retaliation means any act or omission prohibited by law, or which directly or indirectly involves unfavourable treatment that places those who suffer it at a particular disadvantage compared with others in the context of employment or profession, solely because of their status as a whistleblower or because they have made a public disclosure.

Retaliation includes, but is not limited to, retaliation in the form of:

Suspension of the employment contract, dismissal or termination of the employment relationship, including the non-renewal or early termination of a temporary employment contract after the trial period, or the early termination or cancellation of contracts for goods or services, the imposition of any disciplinary measure, demotion or refusal of promotion and any other substantial change in working conditions and the failure to convert a temporary employment contract into a permanent contract, where the employee had a legitimate expectation of being offered permanent employment; unless these measures were taken as part of the normal exercise of management powers under employment legislation, due to

circumstances, facts or proven offences, and unrelated to the presentation of the communication.

Damage, including damage to reputation or economic loss, coercion, intimidation, harassment or ostracism.

Negative assessments or references concerning work or professional performance.

The establishment of a blacklist or the dissemination of information in a particular sectoral area, which hinders or prevents access to employment or the awarding of works or service contracts.

Refusal or withdrawal of a licence or permit.

Refusal of training.

Discrimination or unfavourable or unfair treatment.

6. Archiving of documentation and reports

The LONVIA branch keeps a register of the information received and the internal investigations to which it gives rise, guaranteeing in all cases the confidentiality requirements laid down by law.

Each report contains the following information:

Report date

Date of event

Description

Situation

Resolution, if closed

Other information about the recipient..

All documentation relating to this procedure is kept by the Head of the Internal Information System or the person designated by them for a period of five years or, in any event, for no longer than is necessary for the purposes for which it was processed, in a manner that ensures its confidentiality.

Each year, the Head of the Internal Information System or their representative prepares a summary report on the cases submitted, the analyses performed and the results of these analyses.

The report may contain: (i) an indication of all the reports received, those being analysed and their outcome (archiving, in-depth assessment); (ii) the assessment of the reports accepted and their outcome (archiving, opening of disciplinary proceedings, sanctions applied); and (iii) the proposal of corrective or additional criteria for the procedure.

The register indicated is not public and can only be accessed at the reasoned request of the competent judicial authority, by order, in the context of legal proceedings and under the supervision of that authority.

7. Breaches

The Independent Authority for the Protection of Whistleblowers is the body competent to deal with the breaches referred to in Title IX of Law 2/2023 committed in the public sector of the State.

These breaches include, among others, retaliating against whistleblowers, violating the guarantees of confidentiality and anonymity set out in Law 2/2023 or the obligation to maintain secrecy on any aspect related to the information, as well as communicating or publicly disclosing information in the knowledge that it is false.