ANIMA Holding S.p.A.

Whistleblowing

Document Type	Policy
Version	01
Date of Board Approval	03/11/2023
Date of Application	06/11/2023
Pages	13
Editing and publication	Internal Audit Service and Compliance Service

Contents

Changes to the Document

Versions	Date	Description of Changes
00	09/11/2018	First issue and Board approval
01	03/11/2023	Update for regulatory revision (Legislative Decree 24/2023)

1. Introduction and Overview

This document defines the system to be adopted by Anima Holding (hereinafter also "the Company") for reporting facts or conduct that might constitute a violation, as defined in section 2 - "Terms and definitions".

This document sets out:

- the roles and responsibilities of the bodies and functions to be involved in the handling of reports;
- the subject and requirements of the report;
- the methods and channels of communication that potential whistleblowers can use;
- the analysis phase by the internal whistleblowing officer;
- the reporting phase to the relevant corporate bodies and Supervisory Body.

The process defined below ensures the confidentiality of the whistleblower's identity, on the basis of the relevant rules in force and the internal regulations governing forms of protection against retaliation and/or discrimination against the whistleblower (see section 5 - "Protection systems").

2. Terms and definitions

- **Violations**: conduct, acts or omissions that harm the public interest or the integrity of the company and that consist of:
  - administrative, accounting, civil or criminal offences;
  - unlawful conduct pursuant to Legislative Decree no. 231 of 8 June 2001, or violations of the organisational and management models provided for therein;
  - offences falling within the scope of application of European Union acts in the following areas: public procurement; financial services, products and markets and prevention of money laundering and funding of terrorism; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and animal feed safety and animal health and welfare; public health; consumer protection; privacy and data protection; and network and information systems security;
  - acts or omissions that harm the financial interests of the EU;
  - acts or omissions concerning the internal market, including violations of EU competition and state aid rules, as well as corporate taxes;
  - acts or conduct that frustrate the object or purpose of the provisions of EU acts.

- **Whistleblower:** the natural person who reports information about violations discovered in the context of his/her work context. This individual may be represented by:
  - **employees** and those who work on the basis of relationships that determine their de facto inclusion in the company organisation, even in a form other than an employment relationship;
  - **self-employed workers** as well as those working for the Company in the context of a collaboration;
  - **workers or collaborators**, who carry out their work for the Company by supplying goods or services or carrying out works;
  - **freelancers and consultants** working for the Company;
  - **volunteers and interns,** paid and unpaid, who work for the Company;

- **shareholders and persons with administrative**, management, control, supervisory or representative functions;
- **personnel who have terminated their employment** with the Company if information on the violations was acquired in the course of that employment;
- **persons whose employment relationship has not yet started** ("**candidates**") in cases where information concerning a violation has been acquired during the recruitment process or other stages of pre-contractual negotiations.

- **Reported party**: the party to which the reported violations relate.

- **Internal whistleblowing:** the communication of information about violations submitted through the internal whistleblowing channel referred to in section 4.

- **External whistleblowing:** the communication of information about violations submitted through the external whistleblowing channels referred to in sections 7, 8 and 9.

- **Retaliation:** any conduct, act or omission, even if merely attempted or threatened, implemented as a result of the report, complaint to a judicial or accounting authority or public disclosure, and which causes or may cause the whistleblower or the person who made the complaint, directly or indirectly, to suffer wrongful damage.

3. Regulatory context

This document is drawn up in accordance with the regulatory framework described below.

Legislative Decree no. 24 of 10 March 2023 on the "*Implementation of 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 and on provisions concerning the protection of persons who report breaches of national laws*" (the so-called "Whistleblowing Decree") brings together in a single regulatory text the entire regulations on whistleblowing channels and protections afforded to whistleblowers, taking into account the legislative provisions in force, in order to adopt effective, confidential and secure whistleblowing channels that, at the same time, guarantee effective protection of whistleblowers from possible retaliation.

The Whistleblowing Decree did not repeal the specific sector regulations applicable to AMCs contained in articles 4-*undecies* and 4-*duodecies* of the Consolidated Law on Finance, which provide for (i) the obligation for all intermediaries, including AMCs, to set up internal systems for the reporting by personnel of acts or facts that may constitute a breach of the rules governing business activities as well as of Regulation (EU) no. 596/2014 (the so-called MAR), as well as (ii) specific procedures for reporting to the Supervisory Authorities. Therefore, the relevant implementing rules contained in the "*Bank of Italy implementing regulation of articles 4*-undecies *and 6(1)(b) and c*-bis*) of the Consolidated Law on Finance*" continue to apply to AMCs and, specifically in art. 9, referred to in art. 39, "*Internal Whistleblowing Systems*" under which "*[t]he body with strategic supervisory functions approves the internal whistleblowing violations, in accordance with the provisions of Annex 4"*. Annex 4 governs the characteristics that the internal whistleblowing systems of AMCs must possess.
With reference to the administrative liability of entities, the Whistleblowing Decree amends the original regulations provided for the private sector by Legislative Decree no. 231/2001 "*Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality*", providing that the organisational and management models pursuant to Legislative Decree no. 231/2001

must establish internal reporting channels that meet the requirements of the Whistleblowing Decree, as well as the prohibition on retaliation and the disciplinary system.

Mention should also be made of the anti-money laundering regulation that introduces specific provisions on whistleblowing, through the obligation to report violations of the provisions laid down for the prevention of money laundering and terrorist financing. In particular, art. 48 of Legislative Decree no. 231/2007, as amended by Legislative Decree no. 90 of 25 May 2017, implemented at national level the so-called Fourth (IV) Anti-Money Laundering Directive, which indicates, among other things, that entities subject to the obligation must have reporting procedures in place internally that ensure:

- the protection of the confidentiality of the identity of the whistleblower and of the alleged perpetrator of the violations, and the protection of the whistleblower against retaliation, discrimination or otherwise unfair conduct arising from the report;
- the development of a specific anonymous and independent reporting channel, proportionate to the nature and size of the party subject to the obligation.

The above obligations must be carried out in compliance with the broader legal framework of the General Data Protection Regulation (GDPR), which requires the adoption of appropriate protection measures for the processing of personal data related to each stage of the reporting process.

4. Internal whistleblowing channel

4.1. Internal Whistleblowing Officer (IWO)

The Internal Whistleblowing Officer (IWO) ensures the proper functioning of the whistleblowing process, reports directly and without delay to the corporate bodies on the information reported, where relevant, and draws up an annual report on the proper functioning of the process itself.

A report is considered relevant and therefore deserving of attention by the IWO if it concerns a "violation" (see definition in section 2).
The IWO may not be subordinate to any reported party, may not him/herself be the alleged perpetrator of the breach and may not have a potential interest related to the report such that compromises his/her impartiality and independence of judgement.
If the party to whom the report refers is the IWO, the whistleblowing may submit it to the "back-up" IWO.

IWOs must meet the moral and professional requirements, ensuring utmost impartiality, objectiveness and independence of judgement in the performance of their duties, and must be adequately trained.

The IWO is identified as the Head of the Internal Audit Service and the Head of the Compliance Service as "back-up IWO". Both have been trained in whistleblowing.

If the internal report is submitted to a party other than the competent party, where the whistleblower expressly declares that he/she wishes to benefit from the whistleblowing protections or where this intention can be deduced from the report (e.g. from the use of a specific form for whistleblowing reports or from the reference to the relevant legislation), the report is considered a "whistleblowing report" and must be forwarded by the recipient, within 7 days of its receipt, to the competent internal party, with simultaneous notification of the transmission to the whistleblower.

4.2. Subject and requirements of internal reporting

The report may be:
- confidential: when the whistleblower is known but the Company does not disclose his/her identity without his/her explicit consent;
- anonymous: when the identity of the whistleblower is not made explicit or otherwise identifiable.

Reports must be made in good faith, and personal grievances are not permitted. Such reports will not be considered relevant and will therefore not be investigated by the Internal Whistleblowing Officer.

The report must concern conduct based on precise and concordant facts of which the whistleblower has become aware in his/her work context, i.e. by virtue of the office held or on the occasion and/or as a consequence of performing work duties, even in a casual manner.

The report must be substantiated and specify the facts and conduct in conflict with the legislation, indicating, where possible, the regulatory framework of reference (231/2001, 231/2007, Consolidated Law on Finance, Market Abuse, etc.).

In order to be defined as substantiated, the report must contain the following minimum information:
- a clear and complete description of the facts;
- the time and place in which they occurred;
- the particulars or other elements allowing for the identification of the party who carried out the reported facts;
- any information and/or evidence that might provide valid evidence as to the existence of what has been reported;
- any private interests associated with the report.

4.3. Sending the report

A whistleblower who suspects that a breach has occurred or may occur may send a report for the attention of the Internal Whistleblowing Officer in accordance with the following procedures.

⇒ **For employees**, through one of two alternative channels:
- electronic communication via the "Comunica Whistleblowing" software ("**digital channel");**
- letter by ordinary post ("**paper channel**").

- **For persons outside the Company,** i.e. who do not have access to the Company's systems (suppliers, shareholders, consultants, former employees, etc.), by paper channel.

If the whistleblower considers the IWO to be in conflict with the report, a second recipient, identified as the Head of the Compliance Function, may be specified.

The reporting channels are activated in consultation with any company trade union representatives.

4.3.1. Paper channel

The whistleblower may send a letter to the address of the registered office of Unione Fiduciaria (Via Amedei, 4 – 20123 Milan) for the attention of the Whistleblowing Office – ANIMA.
Upon receipt of the letter, the supplier will send an appropriate communication – by e-mail – to the IWO, who will personally retrieve it within ten working days.

Once the IWO has read the letter, he/she enters the relevant details into the "Comunica Whistleblowing" system (see section 4.3.2) and starts the analysis phase (see section 4.4) or, alternatively, archives the case.

4.3.2. Digital channel

The digital channel is the "Comunica Whistleblowing" platform owned by Unione Fiduciaria.
The platform allows the IWO to monitor the information received in a complete and timely manner and to manage the subsequent stages of reporting.

It also serves as a register of reports (including those received through paper channels) and can be used by the IWO for reporting purposes.

Access to the system by the whistleblower is done anonymously. The whistleblower chooses whether to communicate his/her personal data to the IWO when filling in the whistleblowing form.

In the case of anonymous access and anonymous reporting, the only reference to the report held by the IWO will be a code assigned by the system.

In order to send a whistleblowing report through the digital channel, the whistleblower can access the "Comunica Whistleblowing" system via a link that is also accessible from the company Intranet. To complete access to the Anima whistleblowing page, the whistleblower must enter the company token. The token is valid for six months and it is the responsibility of the IWO to communicate the new replacement token to Unione Fiduciaria and, following confirmation by the supplier, to update the company Intranet.

Once logged into the system, the whistleblower fills in a form containing the necessary questions to substantiate the report, to identify the scope of the report, and attaches any supporting documentation.

Once the form is completed, the system displays a preview, allowing the whistleblower to edit or confirm its contents and send it to the IWO. When sending, the system automatically generates:

- the unique code of the report, which the whistleblower should keep safe in order to consult the progress of the case by the IWO and identify him/herself as the whistleblower;
- the e-mail notifying the IWO about the new report.

4.4. Analysis of the report

The IWO carries out a preliminary examination of whether the prerequisites of substantiation and reliability are met in order to initiate further investigations. Generic reports will not be taken into account.

If the report is deemed to be a mere personal grievance or relates to events already reported and/or known to the Company, or does not fall within the scope of application of the rules governing whistleblowing, the IWO will archive the case and notify the whistleblower.

The IWO may request further clarification from the whistleblower. If the information provided is still insufficient, the IWO will archive the case and notify the whistleblower.

Once the IWO has ascertained that the report is founded, if it relates to one of the following regulatory contexts, the IWO shall promptly inform the relevant parties, if they are not the subject of the report, taking care to omit the whistleblower's details for privacy reasons. The aforesaid contexts include but are not limited to:

1. Market abuse: the IWO informs the Head of the Compliance Function;
2. Corporate liability pursuant to Legislative Decree 231/01: the IWO informs the 231/01 Supervisory Body;
3. Commission of offences for the purposes of Legislative Decree 231/07: the IWO informs the Head of the Anti-Money Laundering Function;
4. Anti-corruption: the IWO informs the Head of the Anti-Corruption Function.

The persons in charge will have the task of coordinating the appropriate investigations to verify the grounds of the report, also making use of external consultants who are competent in the matter under investigation.

4.5. Communications to the whistleblower

The IWO updates the whistleblower on the progress of the case using the same channel as the whistleblower originally used for the report.

Specifically, the following communications by the IWO are envisaged:

- an acknowledgement of receipt must be issued to the whistleblower within 7 days of receipt of the report;
- within 3 months of the date of the acknowledgement of receipt, or, in the absence of such an acknowledgement, within three months of the expiry of the seven-day period from the submission of the report.

"Receipt of the report" is defined as the moment when the IWO:
- collects the paper communication in person;
- receives an e-mail from the "Comunica Whistleblowing" platform notifying him/her of the submission of a new report.

4.6. Internal whistleblowing

With regard to reports received through the digital channel, the IWO can access the dedicated reporting section on the "Comunica Whistleblowing" system.

The IWO prepares an annual report on the proper functioning of the internal whistleblowing systems, containing aggregated information on the findings of the activity carried out as a result of the reports received by the Company and its subsidiaries.

The report is submitted to the Board of Directors and made available to staff on the company Intranet.

4.7. Storage of reports

Reports and related documentation are stored for as long as necessary to process the report and in any case no longer than 5 years from the date of communication of the final outcome of the whistleblowing procedure, in compliance with confidentiality obligations and data storage regulations (GDPR).

4.8. Internal training and information

The whistleblowing policy is available on the company Intranet.

In order to spread awareness and ensure the correct interpretation of the whistleblowing system, adequate training is provided to all staff by the Human Resources Function under the supervision of the Compliance Function.

A copy of this policy is given to new staff upon recruitment.

Clear information on the channel, procedures and prerequisites for making internal reports as well as on the channel, procedures and prerequisites for making external reports are published in a dedicated section on the Company's website.

5. Protection systems

In order to afford greater protection to whistleblowers, so as to encourage them to report offences that have come to their attention in their work context, specific protection measures are envisaged, as governed by the legislation in force.

Protection is also provided:

- when the legal relationship has not yet begun, if information on the violations was acquired during the recruitment process or at other pre-contractual stages;
- during the probation period;
- after the termination of the employment relationship, if information on the violations was acquired in the course of the employment relationship.

These protections also apply in the case of external reporting and public disclosures and are extended to:

- facilitator, i.e. the natural person who assists a whistleblower in the whistleblowing process, operating within the same work context, and whose assistance must be kept confidential; in order to benefit from the protections afforded to the whistleblower, the identity of the facilitator must be disclosed when reporting;

- persons in the same work context as the whistleblower or the person who has made a complaint to the judicial or accounting authorities or the person who has made a public disclosure and who are linked to them by a stable emotional or family relationship up to the fourth degree;
- co-workers of the whistleblower or of the person who has made a complaint to the judicial or accounting authorities or made a public disclosure, who work in the same work context as the whistleblower and who have a habitual and current relationship with that person;
- entities owned by the whistleblower or by the person who made a complaint to the judicial or accounting authorities or made a public disclosure, or for which those same persons work, as well as entities operating in the same work context as the aforementioned persons.

Prohibition on retaliation

Retaliation means any conduct, act or omission, even if merely attempted or threatened, carried out as a result of the report, and which causes or may cause the whistleblower, directly or indirectly, to suffer wrongful damage.

The whistleblower is appropriately protected against retaliation, discrimination and unfair conduct as a consequence of the report, as provided for in the applicable legislation. In the case of shared responsibility, the whistleblower may be subject to preferential treatment compared to the other jointly responsible persons, subject to the applicable regulations.

Support measures

The whistleblower benefits from multiple support measures provided by third-sector entities (including free information, assistance and advice on how to report and on protection from retaliation, on the rights of the interested party, and on the terms and conditions of access to state aid). A list of third-sector entities that provide whistleblowers with support measures is held at the ANAC (Italian National Anti-Corruption Authority).

Protection of confidentiality

In compliance with the reference legislation and in order to foster the dissemination of a culture of legality and encourage the reporting of offences, the Company ensures the confidentiality of the whistleblower's personal data, the confidentiality of the information received by all parties involved in the process, and guarantees that report does not in itself constitute a breach of the obligations arising from the employment relationship.

Reports may not be used beyond what is necessary to adequately follow them up.

In particular, the Company ensures that the whistleblower's identity may not be disclosed without his/her express consent to persons other than those competent to receive or follow up on reports, and all those involved in the handling of the report are required to protect the confidentiality thereof, except in cases where:

- the report is made for the purpose of harm or be otherwise detrimental to the whistleblower (reporting in "bad faith") and there is liability on the grounds of slander or defamation;
- anonymity is not enforceable by law (e.g. criminal investigations, inspections by supervisory bodies, etc.);
- the report reveals facts and/or circumstances such that, although outside the company sphere, make it appropriate and/or an obligation to report to the judicial authority.

Breach of the obligation of confidentiality is grounds for disciplinary liability, without prejudice to any further liability provided for by law.

The Company shall protect the whistleblower from any disciplinary action against him/her if the report proves to be unfounded, except in cases of wilful misconduct or gross negligence. It shall also take all necessary measures to protect the physical integrity and moral character so that the whistleblower is adequately protected against any form of retaliation, penalisation, discrimination or threats.

Reference should be made to the Code of Conduct and the Disciplinary Code for the specific provisions concerning, respectively, the rules of conduct to be followed in relation to whistleblowing, and the disciplinary sanctions provided for in the event of their violation.

6. Forms of protection of the whistleblower

In the analysis phase of the report, pending the ascertainment of possible liability, the whistleblower is protected through:

- confidentiality of personal data; without prejudice to any criminal and disciplinary liability of the whistleblower in the event of an obligation of disclosure, for instance in the event of a request from the judicial authority;
- protection against any discrimination or retaliation;
- protection from accusations by co-workers aimed at damaging their reputation.

7. External whistleblowing procedure

In relation to the violations subject to a report pursuant to Legislative Decree no. 24/23, the whistleblower may make an external report, through the channel activated by ANAC, in one of the following conditions:

1. there is no mandatory activation of the internal whistleblowing channel within his/her work context, or this channel, even if mandatory, is not active or, if activated, does not comply with regulations;
2. the whistleblower has already made an internal report and it was not followed up;
3. the whistleblower has reasonable grounds to believe that, if he/she were to make an internal report, the report would not be effectively followed up or the report might give rise to the risk of retaliation;
4. the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to public interest.

ANAC shall:

- notify the whistleblower of receipt of the report within 7 days from its receipt, unless explicitly requested otherwise by the whistleblower or unless ANAC considers that the notice would undermine the protection of the confidentiality of the whistleblower's identity;
- liaise with the whistleblower and request more information from the latter, if necessary;
- diligently follow up on the reports received;

- carry out the necessary preliminary investigation to follow up on the report, including through hearings and acquiring documents;
- reply to the whistleblower within 3 months or, if there are justified and justified reasons, 6 months from the date of acknowledgement of receipt of the external report or, in the absence of such notice, from the deadline of 7 days from receipt;
- notify the whistleblower of receipt of the report within 7 days from its receipt, unless explicitly requested otherwise by the whistleblower or unless ANAC considers that the notice would undermine the protection of the confidentiality of the whistleblower's identity;
- notify the whistleblower of the final outcome of the report.

The ANAC website provides further guidance on how to submit a report through the external channel.

It should be noted that according to the ANAC Guidelines, an external report concerning violations of the corporate organisational model may not be examined or accepted.

8. Procedures for reporting to the Supervisory Authorities

In order to improve their supervision of intermediaries, the Supervisory Authorities (Bank of Italy, CONSOB) have set up special communication channels to allow the staff of intermediaries to directly send any reports that refer to violations of the regulations of the Consolidated Law on Finance or of EU acts directly applicable to the same subject.
Reports to CONSOB of violations of the Prospectus Regulation as defined in art. 93-*bis*(1)(a) of the Consolidated Law on Finance and violations of Regulation (EU) 596/2014 may be reported by anyone.

9. Public disclosures

Public disclosure means making information about violations publicly available through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people.

The whistleblower benefits from the envisaged protection measures if, at the time of the public disclosure, one of the following conditions is met:

- the whistleblower has previously made an internal and external report, or has made an external report directly and received no response within the required deadlines on the measures envisaged or taken to follow up on reports;
- the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to public interest;
- the whistleblower has reasonable grounds to believe that the external report may involve a risk of retaliation or may not be effectively followed up on due to the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there is a reasonable fear that the recipient of the report may be colluding with or involved in the perpetrator of the violation.