

Antwort.

Antwort Capital S.A.

AIFM Whistleblowing Policy

October 2025

Protocol

Version	Date	Comment	Author	Approved by
1.0	16/07/2024	Initial version	Compliance function	BoD
1.1	16/10/2025	Key updates: Alignment with the Law and GDPR.	Compliance function	BoD

Table of Contents

Table of Contents	2
1 Glossary	2
2 Applicable laws, regulations and directive	4
3 Introduction and purpose	4
4 Personnel responsible for implementation of Policy	4
5 Who is covered by the Policy?	5
6 What can be reported.....	5
7 Legislative protection for whistleblowers	6
8 To whom should a disclosure be made?	7
9 How should a disclosure be made?.....	7
10 Investigation of disclosure	7
11 Confidentiality and processing of data	7
12 Corrective action and arrangements for the communication to the CSSF	8
13 CSSF enforcement measures and legal consequences.....	9
14 Appendix A: Applicable legal framework	9

1 Glossary

Term	Description
AIF	An alternative investment fund managed by the AIFM
AIFM	Antwort Capital S.A., a public limited liability company qualifying and authorized by the CSSF as an alternative investment fund manager under the AIFM Law
AIFM Law	The Luxembourg law of 12 July 2013 on alternative investment fund managers, as amended from time to time
AIFMD	Directive 2011/61/EU on alternative investment fund managers
Board	Board of directors of the AIFM
Board Member(s)	Duly appointed member(s) of the Board of the AIFM.
Company Law	Luxembourg law of 10 August 1915 on commercial companies, as amended
Compliance - CO	The conducting officer of the AIFM responsible for the AIFM's Compliance Function
Conducting Officer(s)	Conducting officer of the AIFM, duly appointed as such by the Board
Complaints Handling Policy	The Complaints Handling Policy of the AIFM
Code of Conduct	The Code of Conduct of the AIFM
Conflict(s) of Interest	Situation where different parties may have interests that might conflict with each other. Such conflicts may arise between different functions and/or units of the AIFM, or between different functions of the AIFM, as well as between one AIF or Investor and another AIF or Investor
Conflicts of Interest Policy	The Conflict of interest policy of the AIFM
Covered Persons	The Law of 16 May 2023 protects whistleblowers working in the private or public sector who acquired information on breaches in a work-related context (current, past or future work-based relationship), including: • the workers (including civil servants and State employees); • the self-employed persons; • the shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including the non-executive members, as well as the volunteers and the paid or unpaid trainees; • any persons working under the supervision and direction of contractors, subcontractors and suppliers. It also protects: • the facilitators (natural person who assists a whistleblower in a confidential manner); • the third persons who are connected with the whistleblowers and who could suffer retaliation, such as colleagues or relatives of the whistleblower; • the legal entities that the whistleblower owns and works for or is otherwise connected with in a work-related context; • the persons who reported or disclosed information on breaches anonymously, but who are subsequently identified and suffer retaliation; • the persons reporting breaches to relevant bodies, offices or agencies of the European Union.

CSSF	<i>Commission de Surveillance du Secteur Financier</i> , the Luxembourg financial supervisory authority of the financial sector
CSSF Circular	The CSSF Circular 18/698 issued by the CSSF on 23 August 2018 regarding authorisation and organisation of Luxembourg investment fund managers
Data Protection Law	Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data
Employees	All members of staff, including senior managers, directors, employees, and trainees, of the AIFM
GDPR	General Data Protection Regulation
Policy	This whistleblowing policy
Senior Management	The conducting officers of the AIFM

2 Applicable laws, regulations and directive

The AIFM will in particular comply with the legal framework stated in Appendix A. New and/or updated regulations might have been issued since the issuance of this document, as such the list might not be up to date. Conversely, the list may contain regulations that are no longer applicable since replaced by new regulation.

3 Introduction and purpose

The AIFM seeks to conduct its business honestly and with integrity at all times. However, we acknowledge that all firms face the risk of their activities going wrong from time to time, or of unknowingly harbouring malpractice. We have a duty to take appropriate measures to identify such situations and attempt to remedy them. By encouraging a culture of openness and accountability within the AIFM, we can help prevent such situations occurring. We expect all Employees to maintain high standards in accordance with our Code of Conduct and to report any wrongdoing that falls short of these fundamental principles. It is the responsibility of all Employees to raise any concerns that they might have about malpractice within the workplace.

This document is the property of the AIFM and is for internal use only by Employees of the AIFM unless otherwise indicated and must not be distributed outside the AIFM. None of the information or images contained in the document may be copied, reproduced, republished or downloaded either in whole or in part to any person or entity outside the AIFM without the written permission of the AIFM.

This Policy is drafted in compliance with paragraph 160 and 260 of CSSF Circular 18/698 and is for the use of the Employees of the AIFM.

Employees should also be aware of the CSSF procedures in respect of whistleblowing which can be consulted on the following link: <https://www.cssf.lu/en/whistleblower-protection/>

What is Whistleblowing?

'Whistleblowing' is the disclosure of information by an Employee or Covered Person which relates to some danger, fraud or other illegal or unethical conduct in the workplace. The aim of this Policy is to ensure that our Employees and Covered Persons are confident that they can raise any matters of genuine concern, without fear of reprisals, in the knowledge that they will be taken seriously and that the matters will be investigated appropriately and regarded as confidential. We encourage all Covered Persons to disclose any concerns which they have about malpractices within the workplace.

4 Personnel responsible for implementation of Policy

The Board has overall responsibility of this Policy but has delegated day-to-day responsibility for monitoring and reviewing the operation of the policy to the Conducting Officer responsible for compliance. The Compliance - CO is responsible for ensuring this policy is kept up to date, within each calendar year, or more frequently if there are material changes in the business, legislation and/or regulation, or risk environment that Employees are trained in how to use this Policy and that procedures are adopted to implement this Policy.

All Covered Persons are responsible for the success of this Policy and should ensure that they take

steps to disclose any wrongdoing or malpractice of which they become aware. If you have any questions about the content or application of this Policy, you should contact the Compliance - CO.

5 Who is covered by the Policy?

This policy applies to all Covered Persons in accordance with the Law of 16 May 2023 transposing the Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law aiming at creating a uniform European legal framework to protect whistleblowers in certain policy areas of the European Union (The Law).

The following persons are not subject to protection:

- the reports of breaches relating to national security;
- the whistleblowers whose relationships are covered by:
 - medical professional privilege;
 - professional privilege between lawyer and client;
 - professional privilege binding notaries or bailiffs;
 - the secrecy of judicial deliberations;
 - the rules governing criminal proceedings.

This Policy will be provided to every Employee when joining Antwort and after any amendment approved by the Board of Directors.

The Policy will be permanently accessible through the AIFM's official corporate website, <https://www.antwort.lu/antwort-regulatory-framework/>, ensuring that all Covered Persons have unrestricted and continuous access to its content. This availability is intended to promote transparency and awareness, allowing individuals to review the Policy at any time, familiarize themselves with the reporting channels, and fully understand their rights and obligations under the established framework.

6 What can be reported

The whistleblower is entitled to report any breach of national and/or European Union law, including acts or omissions that are unlawful or that undermine the object or purpose of directly applicable provisions of national or European legislation. Furthermore, the whistleblower may disclose any information, including reasonable suspicions, concerning actual or potential breaches, as well as attempts to conceal such breaches. These violations may have occurred, be occurring, or be highly likely to occur within the organization where the whistleblower is currently employed or was previously employed, or within another organization with which the whistleblower maintains or has maintained contact in the course of their professional activities.

You should make a disclosure if you have a genuine concern that there are reasonable grounds for believing that any of the following have occurred (non-exhaustive list), are occurring or are likely to occur:

- a criminal offence has been/is about to be committed;
- a person has failed to/not intended to comply with their legal and regulatory obligations;
- a miscarriage of justice has/is about to occurred
- offering or accepting bribes;
- the health and safety of any individual has been/is about to be endangered;
- the environment has been damaged; or

- any of the above are being, or are likely to be, deliberately concealed.

Particular examples of concerns may include acts or omissions that result in:

- illegal activities;
- breach of professional conduct;
- breach of confidentiality;
- the provision of negligent advice;
- financial fraud;
- actions contrary to policy or established procedures or outside the scope of an individual's authority;
- harassment occurring to others;
- activities which result in a Conflict of Interest as described in the Conflict of Interest Policy; and
- activities which endanger health and safety.

This list is not exhaustive and the AIFM will value any report that is made which could be reasonably considered to be in public interest. It is not necessary to have proof that malpractice is being, or is likely to be committed, reasonable belief is sufficient.

The whistleblower may not disclose information acquired or to which he or she obtained access by committing a criminal offence. Furthermore, potentially intrusive information of a personal nature, such as health, political, sexual, or religious beliefs shall not be included in an investigation.

7 Legislative protection for whistleblowers

To qualify for the protection provided under the Law, the whistleblower must meet specific conditions. The individual must have had reasonable grounds to believe, at the time of reporting, that the information concerning the alleged breaches was accurate and that such information falls within the scope of the Law. Additionally, the whistleblower must have submitted the report through one of the recognized channels, namely an internal report using the reporting mechanisms of their enterprise or administration, an external report through the CSSF's designated reporting channels, or, where an external report has proven ineffective, a public report.

No Covered Person who raises genuinely-held concerns under this procedure will be dismissed or subjected to any detriment or victimisation as a result of such action. If you believe that you are being subjected to a detriment within the workplace as a result of raising concerns under this procedure, you should inform the Compliance - CO immediately. Employees are strictly forbidden from mistreating whistleblowers and any Employees who victimise or retaliate against those who have raised concerns under this Policy will be subject to disciplinary action.

An employer is not authorized to retaliate against the person who has filed a complaint or informed the employer of any wrongdoing. Assuming that an Employee is victim of an adverse reaction of the employer, the employer bears the burden of proof to justify that the negative influence on the Employee does not stem from retaliation against a whistleblowing action. Wrongful retaliation gives rise to damages covering the actual loss suffered.

An Employee cannot be victim of reprisals because of his/her protests or refusal opposed to a fact that he/she considers, in good faith, as being constitutive of illegal catch of interests, corruption or influence that this fact is committed by his/her employer or any other senior in rank, colleagues, or external people in relation to the employer (article L.271-1(2) of the Luxembourg Labor Code).

Any termination of the employment contract because of whistleblowing is null and void (article L.271-1 (3) of the Luxembourg Labor Code).

8 To whom should a disclosure be made?

In the first instance, you should raise concerns through the email inbox whistleblowing@antwort.lu owned by the Compliance - CO. In his absence, or where the disclosure is extremely serious or in any way involves the Compliance - CO, you should report the concern to another Board Member.

If the whistleblowing declaration is justified, the Compliance - CO will take the appropriate measures and actions to remedy the detected issue, and, if necessary, submits the report to the Board of Directors of Antwort.

In very serious circumstances or following an internal report which has not been addressed, we recognise that it may be appropriate for you to report your concerns to an external body. The CSSF provides an email address meant for workers who want to report concerns relating to their employer which are relevant to the CSSF's functions (whistleblowing@cssf.lu)

9 How should a disclosure be made?

An internal disclosure should be made to the Compliance - CO either verbally or in writing in English or French. An email that gives details of your concern is all that is needed to initiate this procedure. The Compliance - CO will acknowledge receipt within ten working days of your disclosure and keep a record of further action taken. Any disclosure will be treated in the utmost confidence. You are entitled to make a disclosure anonymously however proper investigation may prove impossible if the investigator cannot obtain further information from you or give you feedback. You are entitled to be accompanied by a workplace colleague or union representative at any meeting with the Compliance - CO under this procedure.

10 Investigation of disclosure

The AIFM is committed to investigating disclosures fully, fairly, quickly and confidentially where circumstances permit. So far as the Compliance - CO is able to legally and practicably handle the disclosure, you will be kept informed of the progress of the investigation. We will aim to deal with all disclosures in a timely manner and with due regard to the rights of all individuals involved. If, after preliminary enquiries have been made, a full investigation is necessary then the AIFM will either investigate internally or refer it to an appropriate external organisation.

Once a report has been made, an acknowledgement of receipt is sent to the whistleblower within seven days.

The whistleblower shall be guaranteed feedback within three months. In compliance with the legal obligation concerning professional secrecy, the AIFM will not disclose to the whistleblower the specific measures implemented in response to the report, except where such measures are subject to disclosure in accordance with applicable legal provisions.

If you are dissatisfied with the investigation or its conclusion, then you should make an external report (see section 8 of this Policy).

11 Confidentiality and processing of data

The AIFM is committed to safeguarding the identity of the whistleblower in accordance with applicable laws. Accordingly, neither the identity of the reporting Employee nor that of any third parties involved will be disclosed without the explicit consent of the whistleblower. The AIFM will not reveal the identity

of the whistleblower or any information from which the whistleblower's identity could be directly or indirectly inferred.

In order to discharge the responsibilities entrusted to it under the Law, particularly in relation to the management and investigation of reports, the AIFM may be required to collect, process, and store personal data. Any such processing of personal data, including the sharing or transfer of information within the scope of the AIFM's duties, is conducted in strict compliance with the GDPR. The AIFM ensures that all personal data are handled securely and lawfully, respecting the principles of data minimization, purpose limitation, and confidentiality, and are processed solely to the extent necessary to fulfill its obligations under the Law and to effectively address and follow up on reported breaches.

Every effort will be made to keep the identity of an individual who makes a disclosure under this Policy confidential. You will also be expected to keep the fact that you have raised a concern, the nature of the concern and the identity of those involved confidential. There may, however, be circumstances in which it will be necessary to disclose your identity, and we will make efforts to inform you that your identity is likely to be disclosed if we believe this is the case.

The Compliance - CO shall conduct the investigation in compliance with the law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data as amended.

Personal data that are clearly irrelevant to the handling of a specific report are neither collected nor, if inadvertently obtained, retained; such data are promptly deleted without undue delay. Similarly, any personal data arising from a report that is assessed by the authorized agents as unfounded or outside the remit of the AIFM are deleted immediately.

Personal data obtained through the reporting process are retained for a period of three months following the closure of the investigation conducted by the AIFM in the discharge of its duties or in connection with proceedings related to the allegations, unless it is necessary to retain them for a longer period in the context of legal proceedings, official investigations, regulatory reporting, or as otherwise required by the AIFM's data protection policy. In such cases, the data will be preserved until the completion of those proceedings or as determined by the applicable internal policies.

Throughout this period, the AIFM ensures that all personal data are securely stored, processed solely for the purpose of addressing and resolving the report, as well as for fulfilling any requirements imposed by the national competent authorities, and handled in full compliance with applicable data protection principles, including confidentiality, integrity, and limited access to authorized personnel only. Upon expiration of the retention period, all personal data are irreversibly deleted to prevent any unauthorized use or disclosure.

12 Corrective action and arrangements for the communication to the CSSF

As part of the investigation into disclosures made under this Policy, recommendations for change will be proposed to enable the AIFM to minimise the risk of the recurrence of any malpractice or impropriety which has been uncovered. The Board will be responsible for reviewing and implementing these recommendations.

The Compliance-CO, together with the other Senior Managers, will prepare a comprehensive list of closing documents as established in Annex 2, point 3 of the CSSF Circular. This package of documents must be submitted within five months following the end of the financial year of the AIFM at the latest, except for the elements specifically requiring submission within one month after the

ordinary general meeting that approved of the annual accounts, and in any case no later than seven months after the financial year-end.

Among the required elements, the list of closing documents will include relevant information related to the handling of reports of infringements of the regulatory framework (whistleblowing).

Once compiled, the list of closing documents will be formally reviewed and approved by the Board of the AIFM. Following approval, the package will be submitted to the CSSF in line with the regulatory requirements, thereby confirming the AIFM's commitment to robust governance, transparency, and ongoing compliance with supervisory expectations.

13 CSSF enforcement measures and legal consequences

In addition to its investigative powers, the CSSF is authorized to impose administrative fines on natural or legal persons who hinder or attempt to hinder a report, refuse to provide information requested by the CSSF in the course of its duties or provide incomplete or false information, breach the confidentiality of whistleblowers, fail to address a reported breach, or neglect to establish internal reporting channels and procedures, including their follow-up, in violation of the Law. These administrative fines range from EUR 1,500 to EUR 250,000, with the maximum amount subject to doubling in the event of a repeat offense within five years from the date of the last final sanction.

Decisions rendered by the CSSF pursuant to the Law may be subject to judicial review before the *Tribunal administratif* (Administrative Tribunal) within one month from the date of notification of such decision.

Furthermore, any whistleblower who knowingly submits or publicly discloses false information may face criminal sanctions, including imprisonment of eight days to three months and a fine ranging from EUR 1,500 to EUR 50,000. In addition, an individual making a false report may incur civil liability, entitling the harmed entity to seek compensation for damages before the competent jurisdiction.

The AIFM maintains a strict zero-tolerance policy toward false reporting and is fully committed to ensuring compliance with the Law and all applicable legal obligations.

14 Appendix A: Applicable legal framework

This Policy should be in line with the following laws, regulations and directives (non-exhaustive list):

- Luxembourg 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.
- Luxembourg code penal
- Luxembourg labour code
- Law of 16 May 2023 transposing the Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law aiming at creating a uniform European legal framework to protect whistleblowers in certain policy areas of the European Union.
- Labour Code, introduced by the Law of 13 February 2011 strengthening the means against corruption, as amended;
- Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data, as amended;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data