



FWU Invest S.A.

Whistleblowing Policy

Revision History

Version	Release Date	Change Description	Owner	Reviewer	Conducting Officer Approval Date	Board of Directors Approval Date
v.1.0	04/2014	Launch, first iteration				
v.2.0	01/2023	Review without material change	Compliance	Compliance Officer	07/02/2023	
v.3.0	02/2024	Re-draft and alignment with the Law of 16 May 2023	Compliance	Chief Compliance Officer		18/03/2024
v.3.1	12/2024	Review, minor update to contact details of authorised agent	Compliance	Compliance Officer	04/12/2024	18/12/2024
v.3.2	04/2025	Change of URL to Whistleblowing Reporting tool	Compliance	Compliance Officer		01/04/2024
v.3.2	12/2025	Review without change	Compliance	CCO	10/12/2025	19/12/2025

Table of Contents

1.	Introduction	3
2.	Applicable Legal Framework	3
3.	Definitions	4
4.	Who is concerned?	5
5.	What can be reported?	5
6.	What conditions shall be met to benefit from the protection granted by the Law of 16 May 2023?	6
7.	Confidentiality	6
8.	Processing of Personal Data	6
8.1	Purpose of the Processing	6
8.2	Period for which the Personal Data will be stored	6
8.3	DPO Contact	7
9.	How should a report be filed with FWU Invest?	7
10.	Procedures for Internal Reporting and Follow-up	7
11.	Public Disclosures	8
12.	Protection against Retaliation	8
12.1	Absence of Liability of Whistleblowers	8
12.2	Prohibited Retaliation Measures.....	8
12.3	Action against Retaliation Measures.....	9
12.4	Reversal of the Burden of Proof.....	9

1. Introduction

FWU Invest S.A. (hereinafter called “the Company”) is committed to the highest standards of openness, probity and accountability.

An important aspect of accountability and transparency is a mechanism to enable staff and other members of the Company to voice concerns in a responsible and effective manner. It is a fundamental term of every contract of employment that an employee will faithfully serve his or her employer and not disclose confidential information about the employer’s affairs. Nevertheless, where an individual discovers information which he/she believes show serious malpractice or wrongdoing within the organisation then this information should be disclosed internally without fear of reprisal, and there should be arrangements to enable this to be done independently of management.

It should be emphasised that this policy is intended to assist individuals who believe they have discovered malpractice or impropriety. It is not designed to question financial or business decisions taken by the Company nor should it be used to reconsider any matters which have already been addressed under harassment, complaint, disciplinary or other procedures. Once the "whistleblowing" procedures are in place, it is reasonable to expect staff to use them rather than air their complaints outside the Company.

This policy serves to implement the Law of 16 May 2023 (“the Law”) transposing 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 which entered into force on 21 May 2023 aiming to guarantee effective and balanced protection for whistleblowers through clearly defined rights and obligations, to reduce the current legal insecurities to which whistleblowers are exposed and, in so doing, to help increase respect for the rule of law.

2. Applicable Legal Framework

In Luxembourg, 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 was transposed by the Law of 16 May 2023 transposing 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 (hereinafter the “Law of 16 May 2023”).

The scope of application of the Law of 16 May 2023 extended the protection of whistleblowers to breaches of national law as a whole. Thus, whistleblowers meeting the conditions of the Law of 16 May 2023 who report breaches of the rules of law, be they administrative or criminal, are therefore protected against any form of retaliation.

The rules applicable to the reporting of potential or actual breaches in the financial sector are currently laid down in the Law of 16 May 2023, which is supplemented by provisions in the following relevant sectoral laws:

- Article 58-1 of the Law of 5 April 1993 on the financial sector, as amended;
- Article 8-3 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended, which was introduced by the Law of 25 March 2020, as amended;
- Article 149b of the Law of 17 December 2010 relating to undertakings for collective investment, as amended;
- Article 23 of Council Regulation (EU) No 1024/2013 of 15 October 2013 (SSM Regulation);
- Title 3 (Articles 36 to 38) of the SSM Framework Regulation;

- Article 8 and of the Law of 23 December 2016 on market abuse, as amended;
- Article 46 of the Law of 30 May 2018 on markets in financial instruments, as amended;
- Article 271-1 et seq. of the Labour Code, introduced by the Law of 13 February 2011 strengthening the means against corruption, as amended;
- Article 10 of the Law of 16 July 2019 on prospectuses for securities.

3. Definitions

For the purpose of this policy, the following definitions apply:

1. **'breaches'** means acts or omissions that:
 - a) are unlawful; or
 - b) defeat the object or the purpose of the directly applicable national or Union rules;
2. **'information on breaches'** means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches;
3. **'report'** or **'to report'** means, the oral or written communication of information on breaches;
4. **'internal reporting'** means the oral or written communication of information on breaches within a legal entity in the private or public sector;
5. **'external reporting'** means the oral or written communication of information on breaches to the competent authorities;
6. **'public disclosure'** or **'to publicly disclose'** means the making of information on breaches available in the public domain;
7. **'reporting person'** or **'whistleblower'** means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities;
8. **'facilitator'** means a natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential;
9. **'work-related context'** means current or past work activities in the public or private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information;
10. **'person concerned'** means a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated;
11. **'retaliation'** means any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person;
12. **'follow-up'** means any action taken by the recipient of a report or any competent authority, to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure;
13. **'feedback'** means the provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up;

14. **‘competent authority’** means any national authority, referred to in Article 18 of the Law, that is designated to receive reports and give feedback to the reporting person, and/or designated to carry out the duties provided for in this law, in particular as regards follow-up;

15. **‘entity’** means any legal entity in the public or private sector, including any entity owned or controlled by such a legal entity in the public sector.

4. Who is concerned?

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;
- 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.

The following 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.

5. What can be reported?

The whistleblower may report any breach of national and/or Union law, i.e. acts or omissions that:

- are unlawful; or
- defeat the object or purpose of directly applicable provisions of national or European law.

The whistleblower may communicate any information, including reasonable suspicions, about:

- actual or potential breaches; and
- attempts to conceal such breaches;

which occurred or are very likely to occur:

- in the organisation in which the whistleblower works or has worked; or
- in another organisation with which the whistleblower is or was in contact through his or her work.

The whistleblower may not disclose information acquired or to which he or she obtained access by committing a criminal offence.

6. What conditions shall be met to benefit from the protection granted by the Law of 16 May 2023?

In order to be protected against any form of retaliation within the meaning of the Law of 16 May 2023, the whistleblower must:

- have had reasonable grounds to believe that the reported information on breaches was true at the time of reporting and that such information falls within the scope of the Law of 16 May 2023; and
- have made either an internal (through the reporting channels of his or her enterprise), an external (through the CSSF's reporting channels) or a public (following an unsuccessful external report) report.

7. Confidentiality

FWU Invest S.A. is committed to protecting the whistleblower's identity within the limits of the applicable laws (ref. to Art. 22 of the Law). In other words, neither the identity of the reporting employee, nor that of any third persons involved will be disclosed beyond the authorised staff members competent to receive or follow up on reports without the explicit consent of the whistleblower.

FWU Invest S.A. will not disclose:

- the identity of the whistleblower without his or her explicit consent;
- any other information from which the identity of the whistleblower may be directly or indirectly deduced.

8. Processing of Personal Data

Any processing of personal data carried out pursuant to the Law shall be carried out in accordance with Regulation (EU) 2016/679 and the Law of 1 August 2018.

8.1 Purpose of the Processing

For the purposes of fulfilling the missions conferred on it by the Law of 16 May 2023, and more precisely concerning the handling of reports, FWU Invest S.A. may need to process personal data.

8.2 Period for which the Personal Data will be stored

Personal data which are manifestly not relevant for the handling of a specific report are not collected or, if accidentally collected, deleted without undue delay.

Personal data obtained through a report that is deemed unjustified by the authorised agents, as it falls outside the FWU Invest's remit, are deleted without delay.

The personal data obtained by means of a report are stored for three months following the closure of the investigation conducted by FWU Invest in the discharge of its relevant tasks or proceedings with respect to the allegations made in the report until the end of the appeal period.

8.3 DPO Contact

Please contact FWU Invest's Data Protection Officer (DPO) for any question regarding the processing of your personal data at the following email address: datenschutzbeauftragter@forwardyou.com

In addition, please read the FWU Invest's Privacy and Data Protection Policy as published in sharepoint.

9. How should a report be filed with FWU Invest?

Any person wishing to report breaches of the law may address FWU Invest in English:

- by using the Whistleblowing Reporting Tool "Hintcatcher" accessible under the following link:
 - <https://report.hintcatcher.com/SXo1OBLB6fd7wu9t14qX/>
- by email to: whistleblowing@fwuinvest.com;
- in person at the head office of FWU Invest;
- by phone: +352 26 19 77 07 or +352 26 19 77 05 during office hours for a first contact.

The form should be the preferred channel as it is the best way of ensuring the independence and autonomy requirements for the receipt and handling of reports received in accordance with Article 17 of the Law of 16 May 2023.

FWU Invest's internal reporting channels ensure the completeness, integrity and confidentiality of the transmitted information. The access to the information thus transmitted is limited to certain authorised FWU Invest agents who are bound to professional secrecy pursuant to Article 16 of the Law of 23 December 1998, which refers to Article 458 of the Criminal Code.

FWU Invest does not record reports made via phone but may draft precise minutes detailing the main elements of the conversation and give the whistleblower the opportunity to verify, rectify and sign them for approval.

In case of reports made via other channels or other FWU Invest staff members, the latter are also bound to secrecy as regards the identity of the whistleblower or the person concerned and transmit the report without delay to the staff members in charge of handling reports.

10. Procedures for Internal Reporting and Follow-up

FWU Invest notably ensures:

- to acknowledge receipt of the report within 7 days of the receipt, unless:
 - explicitly requested otherwise by the whistleblower; or
 - there are reasonable grounds to believe that acknowledging receipt of the report would compromise the protection of the whistleblower's identity;
- to diligently follow up on the report within a reasonable timeframe not exceeding three months from the acknowledgement of receipt or, if no acknowledgement was sent to the reporting person, three months from the expiry of the seven-day period after the report was made.

Due to the legal obligation in respect of professional secrecy under Article 458 of the Criminal Code, FWU Invest will not inform the whistleblower on the concrete measures taken following his or her report, unless these measures will be the object of a disclosure in accordance with the applicable legal provisions.

11. Public Disclosures

A whistleblower who publicly discloses a breach is protected by the Law of 16 May 2023 if:

- the person first reported internally and externally or directly externally, but no appropriate action was taken in response to the report within 3 months following the report; or
- the person has reasonable grounds to believe that:
 - the breach may constitute an imminent or manifest danger to the public interest (e.g. where there is an emergency situation or a risk of irreversible damage);
 - in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach).

12. Protection against Retaliation

12.1 Absence of Liability of Whistleblowers

Whistleblowers who fulfil the conditions for protection do not break the law by disclosing information and do not incur liability of any kind:

- concerning (internal and/or external) reporting or public disclosure provided that they had reasonable grounds to believe that reporting or public disclosure was necessary for revealing a breach of law;
- in respect of the acquisition of or access to the information which is reported or publicly disclosed (unless such acquisition or access constitutes a self-standing criminal offence);
- as a result of reports or public disclosures made, including in legal proceedings for defamation, breach of copyright, breach of secrecy, breach of data protection rules, disclosure of trade secrets, or for compensation claims based on private, public, or on collective labour law.

They have the right to rely on that reporting or public disclosure to seek dismissal of the case.

12.2 Prohibited Retaliation Measures

Any form of retaliation, including threats and attempts of retaliation against whistleblowers resulting from their report, is prohibited.

The following are null and void:

- the suspension of an employment contract, lay-off, dismissal, failure to renew, or early termination of, a temporary employment contract or equivalent measures;
- demotion or withholding of promotion;
- the transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- withholding of training;
- the imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- the failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;

- the negative performance assessment or employment reference;
- the early termination or cancellation of a contract for goods or services;
- the cancellation of a licence or permit;

Are also prohibited:

- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- psychiatric or medical referrals.

12.3 Action against Retaliation Measures

The whistleblower who suffers retaliation measures may, within 15 days following the notification of the measures, request the competent court to declare the measures null and to order them to cease.

The person who has not invoked the nullity of the retaliation measures or who has already obtained their nullity may, furthermore, claim damages.

Persons who take retaliation measures provided for in Article 25 of the Law or bring vexatious proceedings against reporting persons shall be fined between EUR 1,250 and EUR 25,000.

The reporting person who knowingly reported or publicly disclosed false information may face eight days to three months in prison and incur a fine ranging from EUR 1,500 to EUR 50,000.

A person presenting a false report shall bear civil liability. The entity that has suffered damage shall be entitled to claim compensation before the competent court.

12.4 Reversal of the Burden of Proof

The whistleblower who suffers adverse measures automatically benefits from the presumption that these measures have been taken against him or her as a retaliation for the report.