INTERNAL INFORMATION SYSTEM

POLICY AND PROCEDURE

OF

ONE TO ONE ASSET MANAGEMENT, SGEIC, S.A

Internal Information System Policy and Procedure

Table of Contents

1. Introduction and Purpose

The purpose of this policy is to set out the general principles of the Internal Information System and the protection of whistleblowers who report any breach detected at ONEtoONE Asset Management SGEIC, S.A., guaranteeing their protection.

This communication channel gives effect to the obligations imposed by Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption. Through the approval of this law, Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, on the protection of persons who report breaches of Union law, is transposed into Spanish law.

In compliance with Law 2/2023, the Board of Directors of ONE TO ONE ASSET MANAGEMENT SGEIC S.A. approves the Internal Information System Policy, the purpose of which is to define the principles and premises governing the Internal Information System. This System is designed as a tool to strengthen the culture of information/communication as an essential mechanism for the prevention, detection and correction of threats to the public interest and of regulatory breaches, to consolidate the integrity risk oversight framework, and to facilitate compliance with the Code of Conduct in general, and with internal regulations in particular.

ONE TO ONE ASSET MANAGEMENT SGEIC S.A. embraces all the principles set out in Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law and in Law 2/2023 on the protection of whistleblowers, and, in order to emphasise this commitment, approves this Internal Information System Policy.

2. Scope of Application

This Policy provides a level of protection to individuals who, within a work-related or professional context with ONEtoONE, report:

- Acts or omissions that may constitute a serious or very serious criminal or administrative offence. In any case, all serious or very serious criminal or administrative offences that entail economic loss to the Public Treasury or Social Security shall be deemed to be included.
- Acts or omissions that may constitute a breach of European Union law, as defined by Directive (EU) 2019/1937.

Accordingly, communications relating to strictly labour-related matters, human resources policies, or professional performance are excluded from the material scope of application of the internal information system. In such cases, the matter will be referred, where appropriate, to the Human Resources Department.

Likewise, the process for reporting communications through the internal information system must not be used to report events posing an immediate threat to life or property. Where emergency assistance is required, the situation must be reported to the emergency services.

This Policy extends, in addition to the Company's directors, executives and employees, to other collaborators such as interns, workers undergoing training periods, candidates in a selection process, workers whose employment or commercial relationship has ended, as well as to any person working for or under the supervision and direction of clients, contractors, subcontractors and suppliers, and to the Company's partners.

The protective measures provided for in this Policy shall also apply, where applicable:

I. To individuals who, within the organisation in which the whistleblower provides services, assist the whistleblower during the process.

II. To individuals connected to the whistleblower who may suffer retaliation, such as co-workers or relatives of the whistleblower.

III. To legal entities for which the whistleblower works, or with which the whistleblower maintains any other type of relationship in a work-related context, or in which the whistleblower holds a significant interest.

3. Enabled Channels

3.1 Internal Channels

The company has established a confidential, protected Internal Information channel that complies with the requirements of the strictest regulations on the protection of whistleblowers and data protection. This Internal channel is managed through the TRUSTY AG platform, which is accessible via:

- The company's corporate website: https://onetoonefunds.trusty.report/

Communications may also be submitted verbally, by means of an in-person meeting, at the request of the interested party. In such cases, the request must be made through one of the written communication channels mentioned above. Where applicable, the in-person meeting will be held within a maximum period of 7 calendar days from receipt of the communication, in an environment that guarantees confidentiality. The meeting must be duly documented in one of the following ways:

- By recording the conversation in a secure, durable and accessible format, having first informed the whistleblower of the processing of their data in accordance with applicable regulations, or
- By means of a complete and accurate transcript of the conversation prepared by the staff responsible for handling it. In addition, the whistleblower will be given the opportunity to review, correct and approve the transcript of the conversation by signing it.

Communications may be submitted either identified or anonymously.

Communications submitted must contain, as far as possible, the following details:

- Full name of the person(s) to whom the facts and/or conduct reported are attributed.
- Date of the events and the fullest information available about them.
- Any documents or other evidence available that may substantiate the facts and/or conduct reported.

In the event of incompatibility or conflict of interest — i.e. where the person responsible for the reported facts is the person responsible for the Internal Information System — the whistleblower may submit a communication directly, by any means, to Juan Cuesta Diego, who will then provisionally assume, solely for the purposes of managing this breach, the functions of the System's officer.

3.2 External Channels

Without prejudice to access to the internal channels described above, and at any time, any individual who is part of one of the groups with access to the Internal Information System may contact the Independent Whistleblower Protection Authority (A.A.I.) or the corresponding regional authorities or bodies, to report the commission of any acts or omissions falling within the scope of application of Law 2/2023.

The public disclosure or making available to the public of information on acts or omissions within the scope of application of this Policy will also entail protection for the whistleblower, provided that the whistleblower has first reported through internal or external channels, or has reported directly through external channels, without appropriate measures having been taken within the established timeframe, and provided that the requirements set out in the following section are also met.

4. Protection Safeguards

4.1 Data Protection

The exchange or transfer of personal data, as well as any other personal data processed in application of this Policy, will be processed by the Board of Directors of ONE TO ONE ASSET MANAGEMENT SGEIC S.A, with registered office at Zurbarán 7, 1st Floor, 28010 Madrid.

The Company, as data controller, will process the personal data collected through the Internal Information System for the purpose of managing the receipt, recording and analysis of the communications received, as well as for the investigation and resolution of any investigative procedures that may apply. The Company may also process such information in order to maintain a record of the communications received, serving as evidence of regulatory compliance and of the functioning of the system, ensuring that the information is anonymised in this latter case, all of the foregoing based on the obligation arising from Law 2/2023. The processing of special categories of data (sensitive data) will be carried out for reasons of substantial public interest, in accordance with Article 9(2)(g) of Regulation (EU) 2016/679 (GDPR) and Article 30 of Law 2/2023.

The Company will immediately delete any personal data that is not strictly necessary for understanding and investigating the acts or omissions falling within the material scope of this Policy. Likewise, data relating to conduct not covered by Law 2/2023, or data whose inaccuracy has been established, will be deleted, unless such inaccuracy could constitute a criminal offence.

Personal data will be kept in the System only for as long as is strictly necessary to decide whether to initiate an investigation. This period may not, in any case, exceed three (3) months from receipt of the communication, except in cases of particular complexity that justify an extension of up to a further three months.

In order to fulfil the legitimate purposes described above, access to personal data will be limited exclusively to the following recipients, always subject to the legally required confidentiality safeguards:

- The System officer and any third-party service providers acting as data processors (such as legal advisers, experts or external compliance consultants), exclusively where their technical or legal support is strictly necessary for the management, handling and investigation of communications.
- The persons responsible for the Human Resources and Compliance departments, only where imperative for handling the file or for adopting disciplinary or corrective measures. Access will be limited to the information strictly necessary for the performance of their duties.
- Staff performing legal advisory functions for the Company, or those designated by the Company for this purpose, where it is necessary to prepare legal actions or defend the entity's interests in connection with a possible administrative or judicial procedure arising from the investigation.
- Under a legal obligation or for the exercise of public powers, the data may be communicated to:

The Independent Whistleblower Protection Authority (A.A.I.) or, where applicable, the corresponding regional authorities.

The Public Prosecutor's Office and the competent Judicial Authorities, in the event of indications of criminal conduct or in the context of judicial proceedings.

The CNMV (Spanish Securities Market Commission) or other competent Public Administrations in the exercise of their inspection and sanctioning powers.

4.2 Protection of Reporting Persons

Persons who report or disclose infringements falling within the material scope of this Policy will be entitled to the protective measures set out herein, provided the following conditions are met:

- That the whistleblower has reasonable grounds to believe that the information reported is accurate at the time of reporting, and that such information falls within the scope of application of this Policy.
- That the communication has been made in accordance with the channels and formal requirements established by the Company under this information system.

Likewise, protection will be extended to persons who, having made an anonymous communication or public disclosure, are subsequently identified, provided they meet the eligibility requirements described above.

The same right to protection will be afforded to those who report to the competent European Union institutions or bodies in respect of infringements falling within the scope of application of Directive (EU) 2019/1937.

The following will not be covered by this protection:

- Communications that have been rejected for the following reasons:

Where the facts reported are manifestly unfounded.

Where the conduct described does not constitute an infringement of the legal system within the scope of this Policy.

Where there are reasonable grounds to believe that the information was obtained through the commission of a criminal offence. In such a case, the System officer will forward a detailed account of the facts to the Public Prosecutor's Office.

Where the communication does not provide new and significant elements in respect of already concluded proceedings, unless new circumstances of fact or law arise that justify differentiated treatment.

- Information relating to complaints about conflicts of a strictly personal nature or that exclusively affect the whistleblower and the persons concerned.
- Data that is already fully available to the public or that constitutes mere rumour or unsupported speculation.
- Acts or omissions falling outside the objective scope of application of this Policy.

The reasoned decision to reject any communication will be notified to the whistleblower within a maximum period of five (5) working days from its receipt, except in the case of anonymous communications or where the whistleblower has expressly waived the right to receive notifications arising from the procedure.

4.3 Protection Measures for Persons Concerned by the Report

The company will ensure that persons concerned by a communication are heard as part of any internal investigation. It will likewise ensure that they are entitled to a defence, to the presumption of innocence, to the right of defence, and to access to the file, as provided for under applicable law.

Similarly, both the facts reported and the identity of the person concerned by the report of an infringement will be protected and treated confidentially, without prejudice to any appropriate exceptions necessary to ensure the successful outcome of the investigation or any subsequent communication to the competent authorities.

5. Confidentiality

Unless the person making or providing the communication through the Internal Information System expressly consents otherwise, the Company undertakes a full commitment to safeguard that person's identity on the basis of the duty of confidentiality.

This duty of confidentiality ensures that the identity of the whistleblower, as well as any information from which it may be directly or indirectly inferred, will be restricted exclusively to personnel specifically authorised to receive, follow up on and resolve communications. To this end, the Company has implemented the necessary technical and organisational security measures to anonymise information and restrict unauthorised access.

Exceptionally, confidentiality of identity may be lifted only where this constitutes a necessary and proportionate obligation under applicable law, in particular:

- In the context of investigations carried out by competent authorities.
- Within judicial proceedings.

- To safeguard the right of defence of the person concerned.

In such cases, the identity will only be disclosed to the Judicial Authority, the Public Prosecutor's Office, or the competent administrative authority in the exercise of its criminal, disciplinary or sanctioning investigative functions.

Where disclosure of identity is required in accordance with the above, the Company will notify the whistleblower prior to disclosure, unless doing so could jeopardise the success of the investigation or the course of ongoing judicial proceedings.

The Company guarantees confidentiality even where the communication is submitted through unauthorised channels or received by personnel not assigned to the Information System. Staff have been duly instructed on the duty of secrecy and the mandatory obligation to immediately forward any communication to the System officer, and have been warned of the liabilities arising from any breach of such confidentiality.

The Company will ensure that any flow of information to the competent authorities involving trade secrets is handled under strict confidentiality, and will insist that such information is not used or disclosed for purposes other than those strictly necessary for the follow-up of proceedings.

6. Prohibition of Retaliation and Protective Measures

Any act constituting retaliation, in whatever form, including any threat or attempt thereof, is strictly prohibited against persons who submit a communication concerning any of the acts of infringement covered by this Policy, as well as against any person who is or intends to participate in or assist with the investigation process, provided they have acted in good faith and have not participated in the reported act or conduct.

Persons who report acts or omissions falling within the scope of the Internal Information System, or who make a public disclosure thereof, will not be considered to have breached any restriction on the disclosure of information. Consequently, no liability of any kind will arise in connection with such communication or disclosure, provided the whistleblower had reasonable grounds to consider it strictly necessary to clarify the infringement.

Whistleblowers will not incur any liability in respect of the acquisition of, or access to, the information communicated or disclosed, provided that such access or acquisition does not constitute a criminal offence. Where access to the information constitutes an offence, the provisions of applicable criminal law will apply.

Whistleblowers will be entitled to access the support and assistance measures provided for in Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, as well as any applicable guarantees of technical and legal assistance.

7. Register of Communications

The company, at all times ensuring compliance with confidentiality requirements, and for as long as necessary to comply with legal and regulatory requirements, will keep a register of the communications and enquiries received through the Internal Information System.

8. Disciplinary Regime

In compliance with applicable regulations on the protection of whistleblowers, the Company will apply effective, proportionate and dissuasive sanctions, in accordance with the disciplinary regime provided for in the applicable collective bargaining agreement or in applicable labour law, to any members of the organisation who engage in the following conduct:

- Preventing or attempting to prevent the submission of communications, as well as obstructing or attempting to undermine follow-up actions and any subsequent investigation.

- Taking any retaliatory measure, whether direct or indirect, against whistleblowers or persons connected to them.
- Initiating or promoting abusive or bad-faith judicial or administrative proceedings for the sole purpose of harassing the whistleblower.
- Breaching the duty of strict confidentiality regarding the identity of the whistleblower and the persons concerned, or breaching the duty of professional secrecy regarding the content of the communication and any resulting actions.
- Publicly communicating or disclosing information known to be false, or with manifest disregard for the truth (reckless disclosure).