FIDEURAM
ASSET MANAGEMENT IRELAND

RULES ON INTERNAL SYSTEMS FOR REPORTING VIOLATIONS (Whistleblowing)

July 2025

CONTENTS

Document Control

Version n.	Issue date	Issued by	Amendment – whole/partial
1	February 2016	Risks & Compliance	Whole
2	April 2017	Risks & Compliance	Annual review - partial
3	July 2020	Compliance	Whole
4	December 2021	Compliance	Annual review – no changes
5	January 2023	Compliance desk	Annual review – removal of references to the UK Branch, including references to aplicable UK legislation.
6	October 2023	Compliance desk	Review aimed at complying with the Protected Disclosures (Amendment) Act 2022
7	July 2025	Compliance Desk	Review requested by Internal Aduit to align with ISP Rules

1. INTRODUCTION

In compliance with the regulations issued by the Bank of Italy ("Supervisory Provisions for Banks") applicable to the Intesa Sanpaolo Group, as well as the local regulation applicable to FAMI, these Rules contain provisions encouraging employees to report any facts or conduct that would constitute a breach of the rules governing banking activity and any other irregular conduct of which they become aware.

In Ireland, the implementation of Directive 2014/91/EU pursuant to the European Union (Undertakings for Collective Investment in Transferable Securities)(Amendment) Regulations 2016 which amend the European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011 (together the **UCITS Regulations**) has introduced a requirement pursuant to section 25A for UCITS management companies, investment companies and depositaries "to have in place appropriate procedures for their employees to report contraventions of the UCITS Regulations internally though a specific independent and autonomous channel." Fideuram Asset Management (Ireland) dac (**FAMI**) as a UCITS management company is therefore subject to this requirement.

Additionally, the Protected Disclosures Act 2014 provides a framework of statutory protections for whistleblowers in Ireland. The Act has been substantially overhauled by thye Protected Disclosures (Amendment) Act 2022, which came into operation on January 1st, 2023.

An effective internal reporting system (i.e., Whistleblowing) supports the spread of a culture of legality and is an opportunity to improve the business environment both from an organizational and ethical perspective.

The reporting system governed by these Rules ensures the confidentiality of the informant, excluding the risk of punitive, unfair or discriminatory conduct, and fulfils the requirements imposed by the new legislation on employers

Without prejudice to principles/issues governed by the Group's Internal Code of Conduct, this document describes the methods and channels of communication which the informant may use, and the reporting process which take place when a report is submitted. It also indicates the various stages of the process, the persons involved, including their roles and responsibilities, as well as the cases in which the "Head of Internal Reporting System" is required to provide immediate notice to the Corporate Bodies.

1.1 Regulatory References

The main rules requiring the adoption of internal procedures for reporting irregularities or violations of the law are:

at European level:

- Article 71 of Directive 2013/36/EU (CRD IV) on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms;
- Article 32 of Regulation (EU) No. 596/2014 (MAR) on market abuse;
- Article 24 of Regulation (EU) 2015/2365 "Securities Financing Transactions Regulation" (SFTR) on transparency of securities financing transactions and of reuse;

- Article 61 of the Directive 2015/849 (Fourth Anti-Money Laundering Directive) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
- Articles 5 and 25 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of individuals with regard to the processing of personal data, as well as on free movement of such data and which repeals Directive 95/46 /EC
- Article 99(d)(5) of Directive 2014/91/EU amending European Union Directive 2009/65/EU (together the UCITS Directive);

at Irish domestic level:

• Regulation 25A of the European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011 (SI No. 352 of 2011) as amended by European Union (Undertakings for Collective Investment in Transferable Securities)(Amendment) Regulations 2016 (together the **UCITS Regulations**);
• Part 5 of the Central Bank (Supervision and Enforcement) Act 2013);
• Protected Disclosures (Amendment) Act 2022.

1.2 Scope of application

The Rules apply to all employees and external collaborators (such as suppliers and consultants).

2. DESCRIPTION OF THE VIOLATIONS

2.1 Description of the violations subject to reporting

At Group level, all violations of the rules governing banking activities, pursuant to art. 10 of the TUB (Banking Act), thus any related violation related to the savings, (for example, the sale of products or banking services), credit transactions (for example, granting of loans or credit endorsement), financial activities (for example, provision of investment services) as well as any violation relating to activities connected with or instrumental to the bank (such as shareholdings stake) may be subject to reporting.

In the case of FAMI, any member of personnel is asked to report if they have any concerns about any contravention of the UCITS Regulations, possible financial irregularity, malpractice, unauthorized business activity, compliance issue or any other wrongdoing at work including any criminal offence, a failure to comply with legal obligations, a miscarriage of justice, a health and safety risk to individuals, an environmental risk or a concealment of any of these which may impact on FAMI or its shareholder.

The following types of reporting are also included within the scope of Whistleblowing reporting:

- any violation related to Company internal policies and/or procedures, such as the Group's Internal Code of Conduct, the Group Anti-Corruption Guidelines, rules related to procurement, transparency in promoting products and service as well as managing gifts and company expenses;

- any conduct that leads to a conflict of interest arising from the nonobservance of the rules and control procedures for such situations (for example, an employee's conflict in a credit transaction where a personal interest is at stake).

Finally, criminal offenses, such as swindle, embezzlement, theft, corruption, money laundering, self-laundering, extortion, fraud, forgery, insider/internal dealing, inappropriate management of investment portfolios, improper handling of personal data, unauthorized access to IT systems and providing false information to the Authorities may fall within the scope of whistleblowing, if not already included as violations of the rules governing banking activities.

Reporting claims involving interpersonal issues are not included and will follow the dedicated procedures already in place (e.g., line manager, human resources function).

3. PLAYERS INVOLVED

3.1 Reporting person

As prescribed by the Protected Disclosures Act, the following individuals may submit a report: employees and former employees, agency and former workers, current and former contractors, trainees and former trainees, volunteers, board and former board members, shareholders and former shareholders, job applicants.
Reporting persons are properly protected from unfair retaliatory and discriminatory repercussions, and may not lose their job because they have spoken up about unlawful or improper behaviour.
The possibility of adopting special treatment is considered for those informants who may be involved in the violation, consistent with the applicable regulations.

3.2 Head of Internal Reporting System

The Head of Internal Reporting System, who is the Chief Audit Officer, is appointed by the Board of Directors of the Ultimate Parent Company and must ensure the integrity of the process, in compliance with the regulatory provisions.
The Head of Internal Reporting System can delegate all the tasks set out in the following paragraphs to one of the managers in his/her reporting line.
The Head of the Internal Reporting System also performs the reporting activities described in section “4.6 Supervision of the process and Reporting”.

3.3 Delegate

The Delegate shall:

- receive and record the reports submitted;
- acknowledge all reports received within 3 days;
- ensure the confidentiality of the information and the identity of the informant in order to protect him/her from unfair, retaliatory or discriminatory repercussions which may result from the reporting;

- carry out an initial feasibility examination, assessing the conditions to decide whether to proceed with the appropriate investigations or file the report;
- diligently follow up on all reports received;
- depending on the type/scope of the violation, activate the investigations involving the relevant Audit structures or the other competent company Function;
- acquire the results of the investigations conducted by the assigned Function;
- provide feedback to the reporting person on actions taken or envisaged to be taken in follow-up within 3 months;
- provide further feedback to the reporting person at 3 month intervals, on request;
- support the Chief Audit Officer in the preparation of periodic information and the annual report regarding the proper functioning of the systems, which contains aggregate information on the results of the activities undertaken based on the reports received.

3.4 Function responsible for the investigation

The structures of the Chief Compliance Officer Governance Area and/or the Chief Audit Officer and/or other corporate functions identified by the Delegate on the basis of their competence shall proceed with the investigation as indicated in paragraph "4.3 Investigation".

3.5 Human Resources

The competent Human Resources function, engaged by the Function responsible for carrying out the investigation, evaluates and decides, as required by Company regulations, if there are grounds to implement any necessary disciplinary measures and informs the person under investigation if not previously informed.

3.6 Other Operating Functions necessary for remediation

The competent operating Functions, engaged by the function responsible for conducting the investigation, evaluates and implements the necessary risk mitigation measures as defined by the Function responsible for assessment and shared with the audit Function.

4. REPORTING VIOLATIONS

4.1 Reporting

Whenever a reporting person suspects that a violation occurred, or could potentially occur, he/she can report it by sending an email to segnalazioni.violazioni@intesasanpaolo.com to which Chief Audit Officer and its Delegate have an access.
As an alternative, a “backup” channel of communication is available: segnalazioniviolazioni.comitatoperilcontrollo@intesasanpaolo.com which can be used when the reporting person feels that, because of the nature of the report, the Chief Audit Officer structure could potentially be in conflict of interest. In this case, the report shall be addressed to the Management Control Committee that decides on the most appropriate method to carry out the activities usually assigned to the Delegate.
If reports are received via the “backup" channel from employees of the Group Banks/Companies whose audit function is centralised at the Parent, then the Management Control Committee informs the relevant Boards of Statutory Auditors where applicable.

The report should contain a detailed description of the facts and behavior considered in breach of the regulations indicating, if possible, the documents and the rules that are considered violated and other valuable input for conducting the investigation of the alleged offenses.

Appropriate measures will be taken to effectively protect the informant's identity and ensure confidentiality.

The reports are received through specific channels, in a separate and independent manner compared to the ordinary channels.
The employee is obligated to declare if he/she has any personal interest linked to the reporting.

Some persons may wish to make an anonymous disclosure. Anonymous disclosure received will be followed up upon, however, there may be constrained in the ability to investigate the matter in the absence of knowledge of the identity of the reporting person. Further, not having contact information on the identity of the reporting person may make it difficult or impossible to apply certain procedures, such as keeping the reporting person informed on the outcome of their report. If the reporting person does not wish to be contacted, they should make this clear in their report to segnalazioni.violazioni@intesasanpaolo.com or to segnalazioniviolazioni.comitatoperilcontrollo@intesasanpaolo.com.

Where a worker wishes to make a report to the Central Bank under the 2014 Act relating to breaches of financial services legislation by their employer, they may make the disclosure through the following channels:

E-mail: confidential@centralbank.ie

Phone: 1800 130 014 : calls are answered Monday to Friday 9.30am - 5.00pm

Post: Protected Disclosures Desk, Central Bank of Ireland, PO Box 559, Dublin 1.

A person appointed to perform a pre-approval controlled function shall, as soon as it is practicable to do so, disclose to the Central Bank information relating to one or more of the following matters:

(a) that an offence under any provision of financial services legislation may have been or may be being committed;

(b) that a prescribed contravention may have been or may be being committed;

(c) that any other provision of financial services legislation may have been or may be being contravened;

(d) that evidence of any matter which comes within paragraph (a), (b) or (c) above has been, is being or is likely to be deliberately concealed or destroyed,

Reporting persons can also report to the Protected Disclosures Commissioner who will refer the report usually to a suitable regulator, for acknowledgement, follow-up and feedback.

The Office of the Protected Disclosures Commissioner:

E-mail: info@opdc.ie; t disclosures@opdc.ie

Phone: 01 639 5650.

4.2 Receiving, recording and investigation of the report

Upon receiving the report, the Delegate, after viewing it, sends within 3 days, communication to the reporting persont advising him/her of the receipt and registers the report in the dedicated application. The Delegate performs a preliminary analysis of the report and, if necessary, contacts the informant to request any missing documentation.

The relevant reports are then sent to the relevant Function in order to begin with the investigation, while the reports considered irrelevant are filed without any further follow up action, after having advised the informant that the file is considered closed.

The timing of the entire procedure, from the taking in charge of the report till the conclusion of investigations and the consequent release of closing communication of file to the reporting person (see par. 4.4), are necessarily commensurate with the complexity of the checks, however with a duration not exceeding 3 months. This term may be extended if the peculiarities of the detailed case studies require it.
The quarterly reporting to the Management Control Committee of the reports received and the investigations in progress (see par. 4.6) ensures in any case the monitoring of the terms of the process.

4.3 Investigation

The competent Function, identified by the Delegate, shall carry out the investigation, involving the person under investigation for violations that require in depth examination/clarifications, formalizing the findings and the possible need to follow up.

Upon authorization of the Chief Audit Officer, the competent Function contacts the reporting person, if necessary, to request any missing documentation.

- For the assessments requiring follow up action, upon formalization of the findings, the following actions shall be taken:
    - Timely reporting, in the presence of sensitive issues pursuant to Legislative Decree no. 231/01, to the Surveillance Body (SB) of the Company concerned
    - identify together with the competent Operational Functions, any eventual actions of risk mitigation (organizational, IT etc.);
    - involve the Legal Affairs Head Office Department - Group General Counsel any violations committed
    - engage the competent Human Resources Function for any disciplinary actions to be taken
    - report relevant events to the Corporate Bodies; ○ send reports with the results and possible follow up requirements to the Delegate

- The reports regarding investigations without follow up action, are sent to the Delegate for filing.

4.4 Communication to the Reporting person and to the person being investigated

The porting person receives notification when the report has been registered as well as when the file has been closed, once the possibility of following up is evaluated.

The reporting person will be contacted by the person in charge of receiving the report for any basic elements deemed necessary or by the Function that performs the investigation, during the course thereof, upon approval of the Chief Audit Officer.

Regarding the person under investigation, if the findings show critical elements and responsibilities attributed to them, he/she shall be informed of the report and the outcome of the investigation.

4.5 Follow up actions

The Human Resources Function, engaged by the Function that performed the investigation, evaluates whether the conditions for any disciplinary actions exist and, if necessary, proceeds to formally communicate as such, to the person under investigation, specifying that the report stems from whistleblowing.
The relevant Operational Functions, engaged by the function responsible for carrying out the investigation, evaluate and implement the necessary risk mitigation measures (e.g., reinforcement of the processes, controls, systems etc.), as defined by the Function responsible for investigation and shared with the audit Function.

4.6 Supervision of the process and Reporting

The Head of the Internal Reporting System ensures the correct execution of the process in compliance with the regulatory provisions and, in accordance with the regulations on the protection of personal data, updates, on a quarterly basis, the Management Control Committee on the reports received and investigations in progress. He/she also produces an annual report on the proper functioning of the internal reporting systems containing aggregate information on the outcomes of the activities following the reports received, which has to be approved by the Board of Directors and made available to the Bank's personnel.

In the case of significant events, the Chief Audit Officer structure – with the support of other Control Functions if necessary – promptly informs the Managing Director and CEO, the Board of Directors, the Management Control Committee and the Surveillance Body pursuant to the Italian Legislative Decree 231/2001, to the extent of each of their responsibilities.
In addition, as part of the Chief Audit Officer structure periodic reports to the Parent's Surveillance Body and the Companies/Banks with a centralised audit function, summary information is provided to the Surveillance Body of the company in question regarding reports concerning matters relevant for the purposes of Legislative Decree 231/01.
Finally, for Companies whose Audit Function is centralised at the Parent Company, the Chief

Audit Officer structure supplements the periodic report to the Subsidiary's Board of Directors with information on relevant Whistleblowing reports it has received.

4.7 Part 5 of the Central Bank (Supervision and Enforcement) Act, 2013

In the context of a disclosure made by FAMI personnel, where the discloser or the Delegate does not believe that the disclosure has been adequately addressed, or following consideration of the matter by the Function and/or the Board, it is deemed appropriate, a disclosure should be made in accordance with Part 5 of the Central Bank (Supervision and Enforcement) Act 2013 and any such disclosure shall be subject to the provisions of that Act.

5. PROTECTION MEASURES

5.1 Protection of personal data

The Bank implements appropriate safeguards to ensure the confidentiality of personal data for the informant and the alleged violator.

The information and all other personal data acquired through these Rules are treated in compliance with EU Regulation 2016/679 on the protection of personal data, the Code regarding the protection of personal data (Legislative Decree of 30 June 2003, n. 196 and subsequent amendments) and subsequent measures on the same subject ("Privacy Laws and Regulations").

In particular, pursuant to art. 5 and 25 of EU Regulation 2016/679, the personal data processed for the purposes of these Rules must be:

- Adequate, relevant and limited to data strictly necessary to verify the validity of the report and for its management
- treated lawfully, correctly and transparently, calibrating the protection of confidentiality granted to the informant to the one of the person being investigated, in order to protect both from the risks to which, in practice, these subjects are exposed, having particular regard to this aspect when forwarding the report to third parties.

Subjects who receive, examine and evaluate the reports, the Head of the Internal Reporting Systems and any other person involved in the process have an obligation to ensure the confidentiality of information, as well as of the informant identity who, in any case must be protected from retaliatory, discriminatory or otherwise unfair repercussions as a result of reporting.

Pursuant to article 2-undecies of Personal Data Protection Code the rights referred to in articles from 15 to 22 of the EU Regulation 2016/679 by data subjects (including the subjects indicated) cannot be exercised, among others, with a request to the data controller, if the exercise of these rights could result in an actual and concrete prejudice to the confidentiality of the identity of the reporting party. However, the person being reported, alleged perpetrator of the offense, is not precluded in absolute terms from the possibility of exercising the rights provided for by the aforementioned articles of the EU Regulation 2016/679. Indeed, Article. 2-undecies, paragraph 3 of Personal Data Protection Code provides, in relation to the specific limitations to data subjects rights set forth by paragraph 1 of the mentioned article 2-undicies,with reference to the provisions governed by these Rules, which in these cases the rights concerned may be exercised through the Data Protection Authority who balances the right invoked by the person being reported and the need for confidentiality of the informant's identification data. It is understood that in the event of disciplinary proceedings being activated, the identity of the whistleblower cannot be revealed, where the dispute regarding the disciplinary charge is based on separate and additional assessments with respect to the report, even if consequent to the

same. Should the dispute be based, in whole or in part, on the reporting and the knowledge of the informant identity is necessary for defending the accused, the reporting will be usable for disciplinary purposes, only whether the informant released his/her consent to the disclosure of His/her identity.

The identity of the whistleblower may be communicated to the judicial Authority if the latter requires it, in the context of investigations or criminal proceedings started in relation to the facts covered by the report.

All employees have access to the rules for the use and protection of personal data processed in application of these Rules.

5.2 Characteristics and obligations of the persons involved in the process

The persons responsible for receiving, examining and assessing the reports:

- must not be hierarchically and functionally subordinated to the person potentially under investigation;
- cannot be the alleged violator;
- cannot have any potential interest connected to the report which could compromise the impartiality of the decision-making process.

In addition, those persons responsible for the receipt, examination and evaluation of the reports can't participate in the adoption of any decision-making measures, which are assigned to the competent Functions or Corporate Bodies and are bound by the confidentiality obligations included in the previous point.