Breach Reporting Procedure

PG_GRP-004

Procedure Type	Operational
Area	1. Governance Processes
Macro Process	1.3 Audit Processes
Process	1.3.5 Management of Whistleblowing Reports

Editorial	UO Regulation & Processes
Ownership	Internal Audit Department
Approval	Board of Directors
Date of Last Approval	25/06/2026
Issued by	UO Regulation & Processes

TABLE OF CONTENTS

DEFINITIONS

"*Bank*": BFF Bank S.p.A., Parent Company of the Group.

"***Branch***": BFF Bank Sucursal en España, BFF Bank Sucursal em Portugal, BFF Bank Spółka Akcyjna Oddział w Polsce, and BFF Bank SPA Greek Branch. In accordance with Article 4, paragraph 1, point 17, of EU Regulation 575/2013 ("CRR"), a branch is defined as a place of business that constitutes a part of an institution without legal personality and that directly carries out, in whole or in part, the operations inherent to the institution's business.

"***Public disclosure***": for the purposes of this document, this refers to the act of making information on breaches public through the press, electronic media, or any other means of dissemination capable of reaching a large number of people.

"*Group*": the BFF Banking Group.

"*MOG 231*": the Organization and Management Model of BFF Bank S.p.A. and Branches.

"*Corporate Bodies*": the collective body of bodies with strategic oversight, management, and control functions for companies adopting the traditional governance model, the Board of Directors, the Chief Executive Officer, the General Manager; dual governance model (or similar models) the Management Board and the Supervisory Board. Specifically: the Chairman of the Board of Directors, the Board of Directors, the Chief Executive Officer and General Manager, and the Board of Auditors.

"***Supervisory* Body"** or **"SB"**: the body endowed with autonomous powers of initiative and control established by the Bank pursuant to Article 6 of the Decree, tasked with overseeing the operation, compliance, and updating of MOG 231.

"*Head of Breach Reporting System*": the office responsible for managing the internal reporting channel, which must ensure that internal reporting processes and procedures comply with the Decree. The Head of Breach Reporting System is identified as the Supervisory Body of BFF Bank.

"*Feedback*": for the purposes of this document, this refers to the communication to the Whistleblower of information regarding the action taken or intended to be taken in response to the report.

"Retaliation": any conduct, act, or omission-even if merely attempted or threatened-carried out as a result of the report, a complaint filed with judicial or accounting authorities, or public disclosure, and which causes or may cause the Whistleblower or the person who filed the complaint, directly or indirectly, unjust harm.

"Report" or "Internal Reporting": the communication, whether written or oral, of information regarding breaches, submitted through the internal reporting channel. To ensure greater protection, the Group has

decided to allow the use of internal channels also for reports of breaches required by sector-specific regulations.

"***External Reporting***": means a written or oral communication regarding a whistleblowing report submitted through the external reporting channel established by the National Anti-Corruption Authority (ANAC or any other public Authority, in accordance with the applicable laws of each country).

"*Follow-up*": for the purposes of this document, this refers to the action taken by the Head of Breach Reporting System to assess the validity of the reported facts, the outcome of the investigation, and any measures adopted.

"*Internal Breach Reporting System*" (or "*Whistleblowing* System"): for the purposes of this document, this refers to the system designed to allow employees or third parties unrelated to the organizations of the Companies to which this document is addressed to report acts or facts that may constitute a breach of the rules referred to in paragraph 1.5.

"*Reporting Person*" or "*Whistleblower*": the natural person who makes the report or publicly discloses information regarding breaches learned within the context of their work.

"*Person Concerned*": the natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the breach is attributed or as a person otherwise implicated in the breach reported or publicly disclosed.

1 INTERNAL BREACH REPORTING SYSTEM ("WHISTLEBLOWING SYSTEM")

1.1 SUMMARY OF KEY ELEMENTS

HEAD OF BREACH REPORTING SYSTEM	Supervisory Body of BFF Bank S.p.A.
WHO CAN SUBMIT REPORTS	In line with relevant best practices, the Group has identified the following individuals as potential Whistleblowers, specifically: • employees, including all types of employment contracts governed by Legislative Decree 81/2015 (part-time and flexible work; fixed-term work; temporary agency work; apprenticeships; ancillary work) or by Article 54-bis of Decree-Law No. 50 of April 24, 2017, converted with amendments by Law No. 96 of June 21, 2017 (contract for occasional services); • self-employed individuals and those in collaborative arrangements (commercial agency relationships and other types of ongoing and coordinated collaboration); • suppliers of goods and services; • independent professionals and consultants who provide services to the Company; • volunteers and interns, whether paid or unpaid, who provide services to the Company; shareholders and persons holding positions of administration, management, control, supervision, or representation (including de facto positions). • candidates for open positions, if information regarding violations was obtained during the selection process or at other pre-contractual stages, even if the employment relationship has not yet begun.
INTERNAL CHANNEL	The Group has implemented an IT procedure called "Whistleblowing - Reporting of Breaches," accessible via a web link published on the corporate intranet and on the public website, including by subsidiaries and branches. https://digitalplatform.unionefiduciaria.it/whistleblowingnew/en/accessoprincipale/identificazionegruppo?TOKEN=BFFWB This IT procedure allows for reporting in writing or orally via a voice messaging system integrated into the platform.
WHAT CAN BE REPORTED	The following may be reported: • administrative, civil or criminal offenses; • unlawful conduct as defined by Legislative Decree No. 231 of June 8, 2001, or breaches of the BFF Banking Group's Organization, Management, and Control Models and/or Code of Ethics; • offenses falling within the scope of application of the European Union or national acts listed in the annex to Legislative Decree No. 24/2023, or of national acts implementing the European Union acts listed in the annex to Directive (EU) 2019/1937, even if not listed in the annex to Legislative Decree

	No. 24/2023, relating to the following sectors: public procurement; financial services, products, and markets; and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection; and security of network and information systems; • acts or omissions affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union, as specified in the relevant secondary legislation of the European Union; • acts or omissions concerning the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including breaches of European Union competition and state aid rules, as well as breaches concerning the internal market related to acts that breach corporate tax rules or mechanisms intended to obtain a tax advantage that undermines the object or purpose of the applicable corporate tax legislation; • acts or conduct that frustrate the object or purpose of the provisions set forth in Union acts in the sectors indicated in the preceding points; • breaches of European Union restrictive measures referred to in Chapter I-bis, Title I, Book II of the Criminal Code (Articles *275-bis*, *275-ter*, and *275-quater* of the Penal Code), as well as Article 12, paragraph 1-bis, of Legislative Decree No. 286 of July 25, 1998 (provisions against illegal immigration); • breaches of internal anti-corruption regulations; • breaches of the Group's internal regulations (e.g., breaches of corporate policies, procedures, and guidelines) that may implement MOG 231 and/or the BFF Banking Group Code of Ethics, as well as conduct that undermines human dignity.
WHAT CANNOT BE REPORTED	The following may not be the subject of a report, public disclosure, or complaint: • complaints, claims, or requests related to the Reporter's personal interests that pertain exclusively to their individual employment relationships, or that concern their employment relationships with superiors • reports of breaches concerning national defense and security.
CONTENT OF THE REPORT	Reports include all information, including reasonable suspicions, about violations committed or likely to be committed, of which the reporting person becomes aware in the context of their work. Reports must be as detailed as possible, and must clearly state: • the time and place of the reported incident; • a description of the incident; • the personal details or other information necessary to identify the individual responsible for the reported incident.as well as, where possible, be accompanied by documents and the identification of other individuals who may be aware of the facts. Any **anonymous reports**, provided they are specific, detailed, and supported by appropriate documentation, are handled in accordance with this procedure by being recorded in the IT platform by the Head of Breach Reporting System.

	The Bank encourages the indication of the personal details of the Reporting Party in order to apply to them the protections recognized by law and to send them the communications required during the procedure and at its outcome.
PROTECTION MEASURES	The protection system is divided into three categories: • protection of confidentiality and processing of personal data; • protection against any retaliation by the entity in response to the report; • limitations of liability regarding the disclosure and dissemination of certain categories of information.
TO WHOM THE PROTECTION MEASURES APPLY	The protective measures apply to the Whistleblower and the following parties: • facilitators; • persons in the same work environment as the reporting individual, the person who filed a complaint with the Judicial Authority, or the person who made a public disclosure, and who are related to them by a stable emotional bond or kinship up to the fourth degree; • to the work colleagues of the reporting person or the person who filed a complaint with the Judicial Authority or made a public disclosure, who work in the same work environment as said person and who have a regular and ongoing relationship with said person; • entities owned by the reporting person or the person who filed a complaint with the judicial authorities or made a public disclosure, or for which such persons work, as well as entities operating in the same work environment as the aforementioned persons. Whistleblowers are also protected in cases where: • the employment relationship has not yet begun, if the information regarding the violations was obtained during the selection process or other pre-contractual stages; • during the probationary period; • after the termination of the employment relationship, if the information regarding the violations was obtained during the course of the employment relationship itself.
RECEIPT OF THE REPORT	The Head of Breach Reporting System shall notify the Reporter that the report has been acknowledged within **7 (seven)** calendar **days** of its receipt.
FEEDBACK DEADLINE	The Head of Breach Reporting System shall provide feedback to the Whistleblower **within 3 (three) months** from the date of receipt or, in the absence of such notice, within three months from the expiration of the **7 (seven)** calendar **days** period following the submission of the report.
EXTERNAL CHANNEL	As an alternative to internal reporting, the Reporting Person may file an external report through the channel established by the National Anti-Corruption Authority (ANAC) if, at the time of submission, one of the following conditions applies: • the Whistleblower has already filed an internal reporting and it has not been addressed or has not received a feedback within the timeframes set forth in Legislative Decree No. 24/2023;

	• the Whistleblower has reasonable grounds to believe that if they were to file an internal reporting, it would not be effectively followed up or that the report itself could lead to a risk of retaliation; • the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest. Furthermore, the Whistleblower may contact ANAC to report any acts of retaliation suffered. External reports are received by ANAC through the designated channels: online platform, verbal reports, and in-person meetings scheduled within a reasonable timeframe. For more information on the subject of the report and the procedures for filing an external report, please refer to the guidelines provided by ANAC on its official website.
PUBLIC DISCLOSURE	Public disclosure of breaches must occur in accordance with the conditions set forth in Legislative Decree No. 24/2023 so that the Whistleblower may benefit from the protections provided, specifically: • no feedback has been provided to an internal and/or external report within the time limits established by Legislative Decree No. 24/2023; • there are reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest; • there are reasonable grounds to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as those in which evidence may be concealed or destroyed, or in which there is a well-founded fear that the recipient of the report may be colluding with the perpetrator of the breach or involved in the breach itself.

1.2 INTRODUCTION AND CONTENTS OF THIS DOCUMENT

The Whistleblowing policy contained in this procedure applies to **BFF Bank S.p.A.** (hereinafter the "Bank" or the "Parent Company"), including its **Branches**, as well as to its **Italian and foreign Subsidiaries** (hereinafter "Subsidiaries"), which shall formally adopt it and, where justified by local regulatory requirements, shall integrate it taking such requirements into account, as indicated in Annex I.

The Group has established an internal system for reporting breaches pursuant to Legislative Decree No. 24/2023, ("implementing EU Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting on breaches of Union law and laying down provisions on the protection of persons reporting on breaches of national law") to enable the Whistleblower to report any unlawful conduct relevant to the Bank and/or its Subsidiaries and to ensure the protection of confidentiality and protection against retaliation against the Whistleblower and other designated individuals (see above: "to whom the protective measures apply").

This document governs, in accordance with the ANAC Guidelines [1], the key elements of the system adopted and, in particular:

- the Head of Breach Reporting System;
- the Reporting Parties and the subject matter of the reports;
- the protections guaranteed by the system and the parties to whom they apply;
- the channels available for submitting reports;
- the processes for managing reports, including the assignment of related roles and responsibilities.

The process described in this procedure is subject to ex-ante verification by the Compliance & AML Department.

The Group has informed the trade union representatives regarding the implementation and the updating of the breach reporting system.

1.3 HEAD OF BREACH REPORTING SYSTEM

The **Head of Breach Reporting System** was appointed by resolution of the Bank's Board of Directors **within the Supervisory Body of BFF Bank S.p.A**. The same Body is also assigned this role for the Subsidiaries, pursuant to resolutions adopted by the relevant bodies of the Subsidiaries and specific intra-group contractual agreements .

The **Head of Breach Reporting System** must be appropriately trained (see paragraph 2 for further details).

The Supervisory Body is supported by the Group's relevant functions, through the **Head of Internal Audit Function**, who, together with the staff of the Internal Audit Function, constitutes the support structure for the Head of Breach Reporting System. The individuals within the Internal Audit Function called upon to perform a support role for the Head of Breach Reporting System are:

- specifically trained and competent;
- previously and necessarily authorized to process personal data.

The Supervisory Body may request additional funding from the Board of Directors for the management of reports, if it deems it appropriate and provides the necessary justification.

[1] ANAC Guidelines on the Protection of Persons Reporting Breaches of Union Law and the Protection of Persons Reporting Breaches of National Regulatory Provisions. Procedures for the submission and handling of external reports. Approved by Resolution No. 311 of July 12, 2023; ANAC Resolution No. 478 of November 26, 2025, "Guidelines on Whistleblowing via Internal Reporting Channels."

The Head of Breach Reporting System, as well as all **staff** of the support unit or otherwise involved in the report management process, are authorized to process personal data.

In order to address conflicts of interest (actual or potential) that may arise following the submission of a report, it is noted that if the report concerns one of the **members of the Supervisory Board**, the role of Head of the Violation Reporting System will be assigned to the **Head of the Compliance and AML Function.**

The IT procedure automatically forwards the report to the appropriate manager of the Whistleblowing System based on the reporter's indication of a potential conflict of interest.

If the **substitute** is also subject to a conflict of interest, the Reporting Person may contact ANAC through the external channel, provided one of the conditions set forth in Article 6 of Legislative Decree No. 24/2023 applies.

In the event that **reports are received by the Breach Reporting System Manager through a method other than the one indicated, via electronic means** (e.g. email/certified email or regular mail) such reports will be recorded in the IT platform by the Manager, and their handling will be governed by the provisions of this document; the documentation received (digital or paper) must be retained (see paragraph 2.2.4 for further details) and processed in order to protect the confidentiality of the reporting person's identity and the data protection of all data subjects.

Finally, if the internal reporting is submitted to **parties other** than the Officer in charge of the Breach Reporting System and it is clear that it is a whistleblowing report (e.g. the word "Whistleblowing" is explicitly stated on the envelope, in the subject line, or in the text of the communication), it shall be forwarded, **within 7 (seven) days** of receipt and without retaining a copy, to the Head of Breach Reporting System, with simultaneous notification of the forwarding to the Reporting Person.

In the event of **a prolonged absence** (more than two weeks) by the Head of Breach Reporting System, the Head of Compliance & AML Function shall act as a substitute.

1.4 REPORTERS AND THOSE WITH A DUTY TO REPOR

Pursuant to current regulations, reports may be made by the following individuals regarding breaches of which they have become aware within their **work context**[2] :

- employees, including all types of employment contracts governed by Legislative Decree No. 81/2015 (part-time and flexible work; fixed-term work; temporary agency work; apprenticeships; ancillary work) or by Article 54-bis of Decree-Law No. 50 of April 24, 2017, converted with amendments by Law No. 96 of June 21, 2017 (contract for occasional services);
- self-employed individuals and those in collaborative arrangements (commercial agency relationships and other types of ongoing and coordinated collaboration);
- suppliers of goods and services;
- independent professionals and consultants who provide services to the Company;
- volunteers and interns, whether paid or unpaid, who provide services to the Company;
- shareholders and persons holding positions of administration, management, control, supervision, or representation (including de facto positions);
- candidates for open positions, if information regarding violations was obtained during the selection process or at other pre-contractual stages, even if the employment relationship has not yet begun.

1.5 SUBJECT MATTER OF REPORTS

Reports concern information regarding conduct, acts, or omissions of which the Reporter has become aware in the workplace.

By way of example, reports may pertain to:

- administrative, civil, or criminal offenses;
- unlawful conduct as defined by Legislative Decree No. 231 of June 8, 2001, or breaches of the BFF Banking Group's Organization, Management, and Control Models and/or Code of Ethics;
- offenses falling within the scope of application of the European Union or national acts listed in the annex to Legislative Decree No. 24/2023, or of national acts implementing the European Union acts

[2] The definition of "workplace" must necessarily be broad and must therefore include not only employees but also other individuals who have a qualified relationship with the entity/administration, e.g., consultants, volunteers, shareholders, interns, and persons with administrative, managerial, and supervisory functions. Finally, reports may cover facts learned by virtue of the position held, as well as information acquired during and/or as a result of the performance of work duties, even if only incidentally.

listed in the annex to Directive (EU) 2019/1937, even if not listed in the annex to Legislative Decree No. 24/2023, relating to the following sectors: public procurement; financial services, products, and markets; and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection; and security of network and information systems;

- acts or omissions affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union, as specified in the relevant secondary legislation of the European Union;
- acts or omissions concerning the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including breaches of European Union competition and state aid rules, as well as breaches concerning the internal market related to acts that breach corporate tax rules or mechanisms intended to obtain a tax advantage that undermines the object or purpose of the applicable corporate tax legislation;
- acts or conduct that frustrate the object or purpose of the provisions set forth in Union acts in the sectors indicated in the preceding points;
- breaches of European Union restrictive measures referred to in Chapter I-bis, Title I, Book II of the Criminal Code (Articles 275-bis, 275-ter, and 275-quater of the Penal Code), as well as Article 12, paragraph 1-bis, of Legislative Decree No. 286 of July 25, 1998 (provisions against illegal immigration);
- breaches of internal anti-corruption regulations;
- breaches of the Group's internal regulations (e.g., breaches of corporate policies, procedures, and guidelines) that may implement MOG 231 and/or the BFF Banking Group Code of Ethics, as well as conduct that undermines human dignity.

To ensure greater protection, the Group has decided to allow the same internal reporting channel to be used for reporting breaches covered by sector-specific regulations:

- **breaches of the rules governing banking activities,** pursuant to Art. 52-bis "Breach Reporting Systems," Legislative Decree No. 385/1993 (Consolidated Law on Banking and Credit);
- **breach of the regulations governing the prevention of money laundering and terrorist financing,** pursuant to Article 48 "Reporting of Breaches," Legislative Decree No. 231/2007 (Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing);

- **breach of the regulations governing financial activities,** pursuant to Article 4-undecies "Internal systems for reporting breaches," Legislative Decree No. 58/1998 (Consolidated Law on Financial Intermediation).

1.6 CONTENTS OF THE REPORT

Reports should cover all information, including reasonable suspicions, regarding violations that have been committed or may be committed, of which the reporter has become aware in the course of their work.

Reports must be as detailed as possible and must therefore clearly state:

- the time and place where the incident described in the report occurred;
- description of the incident;
- the personal details or other information necessary to identify the individual responsible for the reported incident, as well as, where possible, be accompanied by documents and the identification of other individuals who may be aware of the facts. The Group encourages the disclosure of the Whistleblower's personal details in order to apply the protections afforded by law and to send them the communications required during the proceedings and upon their conclusion.

However, the Whistleblower may remain anonymous if they deem it appropriate In this case, the Whistleblower will not receive a unique report code and therefore will not be able to track the progress of the case or receive feedback or follow-up communications. However, if the Whistleblower is subsequently identified and suffers retaliation, they will be eligible for the protective measures provided by law (Article 16, paragraph 4, of Legislative Decree No. 24/2023).

Therefore, any **anonymous reports**, provided they are specific, detailed, and supported by appropriate documentation, are handled in accordance with this procedure by being recorded in the IT platform by the Head of Breaches Reporting System. The documentation received must be retained.

Finally, reports should not contain special categories of personal data as defined in Article 9 of the GDPR (information revealing racial or ethnic origin, religious, philosophical, or other beliefs, political opinions, membership in political parties, trade unions, associations, or organizations of a religious, philosophical, political, or trade union nature, as well as personal data revealing health or sex life) or criminal data as defined by Article 10 of the GDPR (personal data relating to criminal convictions and offenses or related security measures). If reports contain the aforementioned categories of personal data, whether relating to

the reporter or to third parties, such data will be deleted, unless there are retention obligations or such retention is authorized by law or by a decision of the competent Data Protection Authority.

1.7 CONTENT EXCLUDED FROM REPORTING

The following may not be the subject of a report, public disclosure, or complaint:

- complaints, claims, or requests related to the personal interests of the Reporting Person that pertain exclusively to their individual employment relationships, or that concern their employment relationships with superiors;
- reports of breaches concerning national defense and security.

1.8 PROTECTIONS GUARANTEED BY THE BREACH REPORTING SYSTEM

The **protection system** is divided into three categories:

- protection of confidentiality and processing of personal data;
- protection against any retaliation by the organization resulting from the report;
- limitations on liability regarding the disclosure and dissemination of certain categories of information.

The Group has established appropriate **safeguards to protect the Whistleblower and any individuals involved in the reporting process in various capacities**, who, precisely because of the role they play in the reporting process and/or the specific relationship they have with the Whistleblower, could be subject to retaliation.

The protective measures apply to the Whistleblower and the following parties:

- facilitators[3] ;
- persons in the same work environment as the Whistleblower, the person who filed a complaint with the Judicial Authority, or the person who made a public disclosure, and who are related to them by a stable emotional bond or kinship up to the fourth degree;
- to the work colleagues of the reporting person or the person who filed a complaint with the Judicial Authority or made a public disclosure, who work in the same work environment as said person and who have a regular and ongoing relationship with said person;

[3] The Facilitator is the individual who assists the Whistleblower in the reporting process, operates within the same workplace, and whose assistance must be kept confidential.

- entities owned by the reporting person or the person who filed a complaint with the judicial authorities or made a public disclosure, or for which such persons work, as well as entities operating in the same work environment as the aforementioned persons.

Whistleblowers are also protected in cases where:

- the employment relationship has not yet begun, if the information regarding the violations was obtained during the selection process or other pre-contractual stages;
- during the probationary period;
- after the termination of the employment relationship, if the information regarding the violations was obtained during the course of the employment relationship itself.

1.8.1 PRIVACY PROTECTION AND PROCESSING OF PERSONAL DATA.

The Group guarantees the confidentiality of the personal data of the Whistleblower and of all parties involved in the report.

In particular, the identity and any other information from which the identity may, even indirectly, be inferred, may not be disclosed to persons other than the Head of Breach Reporting System and those authorized to process the Whistleblower's personal data for the purpose of following up on the report . The protection of confidentiality also applies to the content of the reports and related documentation.

With regard to the receipt and handling of reports of violations pursuant to Legislative Decree 24/2023, please note that:

- The **Data Controller** is BFF Bank S.p.A., both with respect to the report and the subsequent actions taken.
- Joint **Data Controllers** are the subsidiaries of BFF Bank S.p.A. that outsource the management of internal reporting channels pursuant to the aforementioned procedure;
- The **Data Processor**, on the other hand, is Unione Fiduciaria S.p.A., acting as a third-party provider of the IT platform pursuant to Article 28 of EU Regulation 2016/679.
- **Authorized to process data** are the Manager of the Violation Reporting System, as well as all staff of the support structure or otherwise involved in the report management process, and the Supervisory Boards of the Italian subsidiaries.

Should it become necessary for any reason to disclose the Whistleblower's identity, a written notice will be provided to the Whistleblower explaining the reasons for the disclosure, and the Whistleblower's express consent must be obtained before proceeding. If the Whistleblower refuses to give consent, the decision to

continue or discontinue the handling of the report will be evaluated in accordance with applicable regulations.

The Whistleblower is informed in advance about the processing of personal data through a specific privacy notice published on the IT platform dedicated to reports and on the institutional website of the Bank and of each Branch and Group Company in the section regarding Whistleblowing. This notice generally contains the following elements:

- the purposes and legal basis of the processing;
- any recipients or categories of recipients of the personal data;
- where applicable, the transfer of personal data to a third country;
- whether the provision of such data is mandatory or optional;
- the data subject's rights pursuant to Articles 15–22 of Regulation (EU) 2016/679;
- the identification details of the Data Controller and the contact information of the Data Protection Officer;
- the right to lodge a complaint with a supervisory authority;
- the retention period for the data provided with the report.

A data protection impact assessment has been conducted in accordance with Article 35 of the GDPR for all legal entities within the group. Personnel involved in managing reports are authorized to process the data.

1.8.2 PROTECTION AGAINST RETALIATION.

The Group, in promoting a work environment that fosters open communication, ensures protective measures for individuals who make whistleblowing reports in good faith and for others involved in the report, safeguarding them from any retaliation or discrimination related to the report made, and ensuring that such action does not adversely affect their ongoing relationship with the Group.

In particular, any act of retaliation or discrimination against Whistleblowers is prohibited and, if established, may lead to disciplinary proceedings against the responsible party and to sanctions and administrative proceedings by the Authorities in accordance with regulatory provisions. Retaliation is also prohibited if it is indirectly linked to the report .

Whistleblowers and the other entities mentioned above may report to ANAC any retaliation they believe they have suffered. The competent judicial authority shall adopt all necessary measures, including

provisional ones, to ensure the protection of the legal rights asserted, including compensation for damages, reinstatement to the workplace, an order to cease conduct in breach of the prohibition against retaliation, and a declaration of nullity of acts adopted in breach of said prohibition.

Retaliatory conduct includes:

- dismissal, suspension, or equivalent measures;
- demotion or failure to promote; denial of an employee's promotion;
- a change in duties, a change in the workplace, a reduction in salary, or an unfavorable change in working hours;
- suspension of training or any restriction on access to it;
- negative performance reviews or negative references;
- the imposition of disciplinary measures or other sanctions, including financial penalties;
- coercion, intimidation, harassment, or ostracism;
- discrimination or otherwise unfavorable treatment;
- failure to convert a fixed-term employment contract into a permanent employment contract, where the employee had a legitimate expectation of such conversion;
- the failure to renew or the early termination of a fixed-term employment contract;
- damages, including to the person's reputation, particularly on social media, or economic or financial harm, including the loss of economic opportunities and loss of income;
- inclusion on blacklists based on a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in that sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the revocation of a license or permit;
- a request to undergo psychiatric or medical examinations;
- a negative performance evaluation or an opinion on the quality of work.

The definition of retaliation covers not only cases where retaliation has already occurred, but also those where it is merely "attempted" or "threatened."

The application of the protection against retaliation regime provided for by the decree is subject to certain conditions and requirements:

- the Whistleblower reported, filed a complaint, or made a public disclosure based on a reasonable belief (reasonable grounds) that the information regarding the reported, disclosed, or complained-about breaches is truthful and falls within the objective scope of application of the decree;

- the report or public disclosure was made in compliance with the provisions of Legislative Decree 24/2023;
- there must be a causal link between the report, disclosure, or complaint made and the retaliatory measures suffered;
- it is not sufficient to report mere suspicions or "rumors."

The reasons that led the person to report, file a complaint, or make a public disclosure are irrelevant for the purposes of their protection.

In the absence of these conditions:

- reports, public disclosures, and complaints do not fall within the scope of the whistleblowing regulations, and therefore the protection provided does not apply to those who report, file a complaint, or make a public disclosure;
- similarly, protection is excluded for other individuals who, due to their role in the reporting/complaint process and/or their particular relationship with the reporter or complainant, indirectly suffer retaliation.

Entities and individuals to whom the protections apply may report to ANAC any retaliation they believe they have suffered. In the event of retaliation occurring in the workplace, ANAC notifies the National Labor Inspectorate for measures within its jurisdiction.

1.8.3 LIMITATIONS OF LIABILITY FOR THOSE WHO REPORT, FILE COMPLAINTS, OR MAKE PUBLIC DISCLOSURES

The Whistleblower, as well as the other protected individuals indicated above, shall not incur any civil, criminal, or administrative liability for:

- disclosure and use of official secrets (Art. 326 of the Italian Criminal Code);
- disclosure of professional secrets (Art. 622 of the Italian Criminal Code);
- disclosure of scientific and industrial secrets (Art. 623 of the Italian Criminal Code);
- breach of the duty of fidelity and loyalty (Art. 2105 of the Civil Code);
- breach of provisions relating to copyright protection;
- breach of provisions regarding the protection of personal data;
- disclosure or dissemination of information regarding breaches that damage the reputation of the person concerned.

This limitation of liability applies if the following conditions are met:

- that at the time of disclosure or dissemination, there are reasonable grounds to believe that the information is necessary to uncover the breach. The person must therefore reasonably believe -and not merely speculate - that such information must be disclosed because it is indispensable for bringing the breach to light, excluding any superfluous details, and not for additional or different reasons (e.g., gossip, vindictive, opportunistic, or sensationalist purposes);
- that the report, public disclosure, or complaint was made in accordance with the conditions set forth in Legislative Decree No. 24/2023 in order to qualify for protection against retaliation (reasonable grounds to believe that the information regarding the breaches was accurate and fell within the scope of reportable breaches under Legislative Decree No. 24/2023); internal and external reports, and public disclosures made in compliance with the procedures and conditions set forth in Chapter II of Legislative Decree No. 24/2023.

Furthermore, unless the act constitutes a criminal offense, the Whistleblower shall not incur any liability, including civil or administrative liability, for obtaining information regarding breaches or for accessing such information. However, if the acquisition constitutes a criminal offense, e.g., unauthorized access to a computer system, the criminal liability and any other civil, administrative, and disciplinary liability of the Whistleblower shall remain unaffected.

In any case, criminal liability and any other liability, including civil liability, is not excluded for conduct, acts, or omissions not related to the report, the complaint to the judicial authorities, or public disclosure, or that are not strictly necessary to reveal the breach.

1.9 SANCTION SYSTEM

ANAC imposes the following administrative monetary sanctions on the perpetrator of the violation:

a) from 10,000 to 50,000 euros when it determines that the natural person identified as responsible has engaged in retaliation;

b) from 10,000 to 50,000 euros when it determines that the natural person identified as responsible has obstructed the report or attempted to obstruct it;

c) from 10,000 to 50,000 euros when it determines that the natural person identified as responsible has breach the confidentiality obligation referred to in Article 12 of Legislative Decree No. 24/2023. This is

without prejudice to the sanctions applicable by the Data Protection Authority for matters within its jurisdiction under the regulations governing personal data;

d) from 10,000 to 50,000 euros when it determines that no reporting channels have been established; in such cases, the Board of Directors is liable;

e) from 10,000 to 50,000 euros when it determines that procedures for handling and managing reports have not been adopted or that the adoption of such procedures does not comply with the provisions of the decree; in such cases, the Board of Directors is held liable;

f) from 10,000 to 50,000 euros when it is determined that the reports received have not been reviewed and analyzed; in such cases, the Head of Breach Reporting System is held liable;

g) from 500 to 2,500 euros, when it is established, even by a first-instance judgment, the civil liability of the reporting person for defamation or slander in cases of willful misconduct or gross negligence, unless the same person has already been convicted, even in the first instance, for the crimes of defamation or slander or, in any case, for the same crimes committed through the report to the Judicial Authority.

Finally, the Group will impose disciplinary sanctions on those responsible for the violations described above, as provided for in paragraph 8 of the General Provisions of the 231 Compliance Model.

1.10 SCOPE OF THE PROCEDURE

This procedure applies to the following entities/Group Companies/Branches.

BFF BANK	FOS	BRANCH	SUBSIDIARIES
X	X	Portuguese Branch Spanish Branch Polish Branch Greek Branch	BFF Real Estate (Italy) BFF TechLab (Italy) BFF Finance Iberia (Spain) BFF Polska (Poland) BFF Medfinance (Poland) Debt-Rnt sp. z o.o. (Poland) Komunalny Fundusz Inwestycyjny Zamknięty (Poland) Medico (Poland) Karnowski Law Firm (Poland)

			Restructuring Law Firm Karnowski (Poland) BFF Czech Republic (Czech Republic) BFF Central Europe (Slovak Republic)

The document is available in **Italian** and **English.**

1.11 PARTIES INVOLVED

COMPANY	DEPARTMENT/FUNCTION	ORGANIZATIONAL UNIT
BFF BANK	Chairman of the Board of Directors	N/A
	Chief Executive Officer and General Manager	N/A
	Board of Auditors	N/A
	Supervisory Body	N/A
	Internal Audit Function	N/A
	Human Resources & Organizational Development Function	N/A
	Compliance & AML Department	N/A

1.12 ND REGULATORY REFERENCES

Internal Regulations

- MOG 231 of BFF Bank S.p.A.;
- BFF Banking Group Code of Ethics.

External Regulations

- EU Directive 2019/1937;
- Legislative Decree No. 24 of March 10, 2023;
- Legislative Decree No. 385 of September 1, 1993;
- Legislative Decree No. 231 of November 21, 2007;
- Legislative Decree No. 58 of February 24, 1998;
- Legislative Decree No. 231 of June 8, 2001;
- ANAC Resolution No. 469 of June 9, 2021, "Guidelines on the protection of persons reporting crimes or irregularities of which they have become aware by virtue of an employment relationship, pursuant to Article 54-bis of Legislative Decree No. 165/2001 (so-called Whistleblowing);
- ANAC Resolution No. 478 of November 26, 2025, "Guidelines on Whistleblowing via Internal Reporting Channels";

- ANAC Guidelines on the protection of persons reporting breaches of Union law and the protection of persons reporting breaches of national regulatory provisions – procedures for the submission and management of external reports" (approved by Resolution No. 311 of July 12, 2023);
- Spanish Law No. 2/2023 of February 20, 2023, on the protection of persons reporting regulatory breaches and on the fight against corruption;
- Recommendation No. 1/2026 of the Independent Authority for the Protection of Whistleblowers regarding the design and implementation of an internal reporting system, published on January 14, 2026;
- Portuguese Law No. 93/2021 of December 20, 2021, on the general regime for the protection of Whistleblowers;
- Polish Law No. 928/2024 of June 14, 2024, on the protection of Whistleblowers;
- Greek Law No. 4990/2022 of November 15, 2022, on the protection of persons reporting breaches of EU law;
- Czech Republic Act No. 171/2023 of June 15, 2023, on the protection of Whistleblowers;
- Law of the Slovak Republic No. 54/2019 of September 1, 2023, on the protection of Whistleblowers.

With regard to the Group's Subsidiaries and foreign Branches, **Annex 1** sets forth the specific provisions under their respective local laws which supplement this procedure.

1.13 APPLICATION SYSTEMS

The list of application systems supporting the activities described in the Procedure is available at the following links.

Systems	Whistleblowing Platform – Unione Fiduciaria https://digitalplatform.unionefiduciaria.it/whistleblowingnew/en/accessoprincipale/identificazionegruppo?TOKEN=BFFWB

1.14 UPDATES

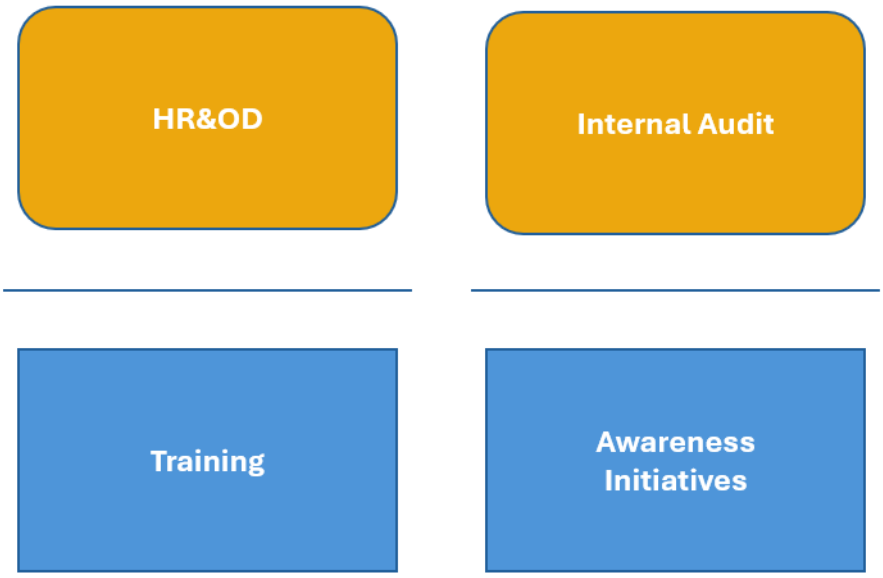
Date and Description	
03/26/2025	Update. The report management process has been modified in light of current regulatory changes (Section 1.9). Additionally, in 2024, several updates were made to the platform used for submitting and managing reports.
06/25/2026	Update. The process for handling reports has been modified to implement the Board of Directors' resolution dated June 26, 2025, which designates the Parent Company's Supervisory Body as the Officer in Charge of the Whistleblowing System.

2 PROCESS

The **Whistleblowing Report Management** Process consists of the following phases:

Training and Awareness	This sub-process describes the parties and activities involved in the following: • Onboarding and ongoing training; 1. Methods for delivering training courses; 2. Awareness initiatives.
Report Management	This sub-process describes the stakeholders and activities involved in the following tasks: 1. Submission of reports; 2. Analysis of the report by the Head of Breach Reporting System; 3. Outcome of the investigation; 4. Archiving of the report; 5. Periodic reporting and report registry.

2.1 TRAINING AND AWARENESS



Staff training is considered essential for the procedure to function effectively. To this end, courses are scheduled periodically, including those conducted by qualified third-party professionals.

The Group informs staff and external collaborators about this procedure and the related privacy notices available on the online platform. To this end, training initiatives and periodic reminders regarding the possibility of submitting whistleblowing reports are provided for Group staff.

Furthermore, this procedure is distributed to staff and made available on the corporate intranet and on the Bank's public website.

2.1.1 INFORMATION AND TRAINING DURING ONBOARDING AND ON-THE-JOB

Owner: **Human Resources & Organizational Development Department**

The Human Resources & Organizational Development Department (through the respective local HR representative), during onboarding, informs new employees of the existence of the breach reporting system by providing this procedure (including in electronic format) and collecting acknowledgment of receipt.

Employees are informed, as part of periodic training, about the purposes of this procedure, the reporting procedures, and the report management process, as well as their rights as data subjects (Articles 15 - 22 of the GDPR) for all legal entities of the Group and the limitations applicable to the individual named in a

report, with particular reference to the protection of the reporter's identity, in accordance with annual plans defined with the Compliance & AML Function.

Specific training, to be periodically updated in accordance with Article 4, paragraph 2, of Legislative Decree No. 24/2023, must be provided to individuals assigned to or involved in the report management process, with the aim of equipping them with the fundamental skills necessary to effectively implement and manage whistleblowing processes, as well as knowledge of the main issues covered by the reports.

These individuals will receive detailed training on the regulations governing the system and the various obligations related to the management of reports, so that they can operate independently and professionally.

>> Control C1: Verification of Training Completion <<

The Human Resources & Organizational Development Department (through the respective local HR contact) verifies that all employees have returned the acknowledgment form for the procedure and monitors the completion of training, establishing an escalation process in the event the course is not completed.

The Human Resources & Organizational Development Department, through the online training platform, records training compliance related to the onboarding phase of new employees and subsequent training sessions, in order to maintain an accurate record of the training conducted, even in the event of significant changes to the platform's functionality, updates to the procedure, or changes to the privacy policy.

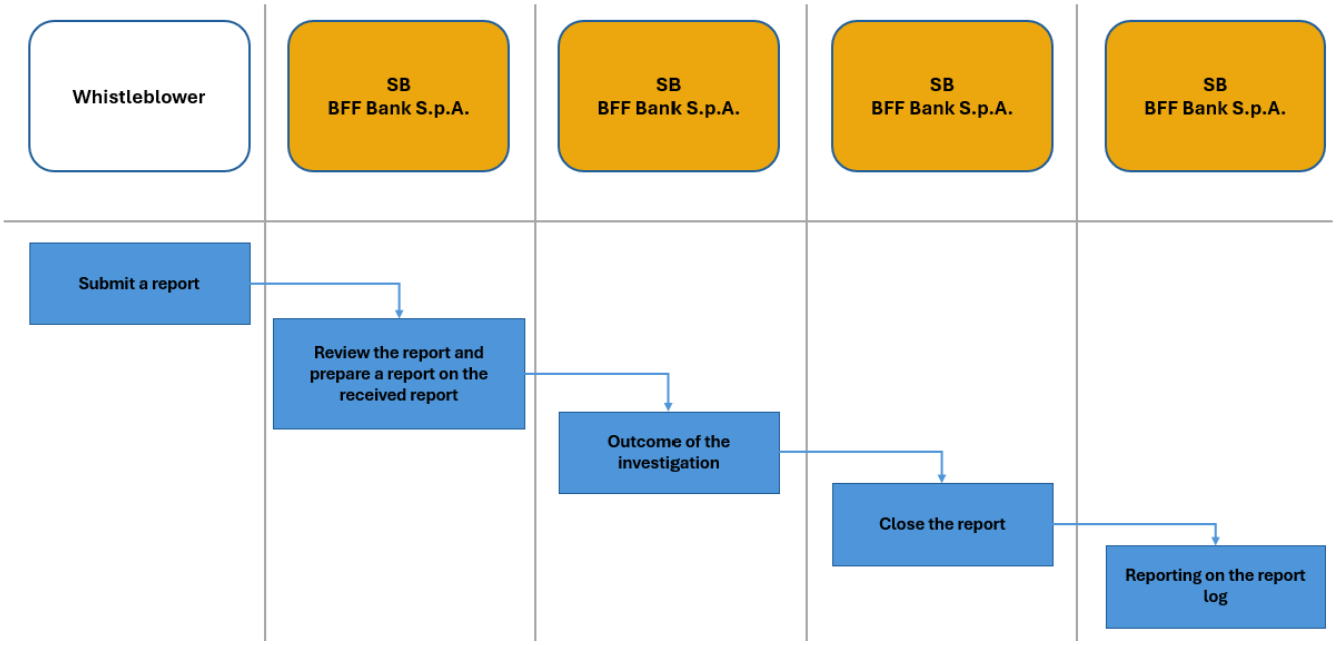
For in-person courses, the Human Resources & Organizational Development Department records and retains attendance records using digital logs (e.g., Excel spreadsheets) or ad hoc paper records.

2.1.2 AWARENESS AND INITIATIVES

Owner **Human Resources & Organizational Development Department and Compliance & AML Department**

- This procedure is made available to employees and external collaborators through publication on the company intranet and the Bank's public website;
- Staff periodically receive awareness emails informing them about the current procedure.

2.2 REPORT MANAGEMENT



2.2.1 SUBMITTING A REPORT

Owner: ***Whistleblower***

Reports may be submitted by the reporting via an IT procedure in either written or oral form.

The Group has implemented an **IT procedure** called "*Whistleblowing – Reporting of Breaches*," accessible via a web link published on the corporate intranet and on the public website:

https://digitalplatform.unionefiduciaria.it/whistleblowingnew/en/accessoprincipale/identificazionegruppo?TOKEN=BFFWB

This online procedure allows users to submit **reports in writing** via text or **verbally** through a voice messaging system integrated into the platform. The procedure is managed by an external provider and guarantees (should the Whistleblower wish to remain anonymous) the anonymity and confidentiality of the Whistleblower's identity, the identity of the person concerned and/or any person mentioned in the report, as well as the content of the report and related documentation.

As expected, privacy safeguards are applied as identified by the DPIA in accordance with Article 35 of the GDPR, and the external provider is duly authorized to process the data pursuant to Article 28 of the GDPR. This IT procedure includes data encryption. Access to the information database by the external provider may occur only for maintenance purposes upon specific authorization and, in any case, without direct access

to the encrypted data. Upon completion of the report, the Reporter is provided with a unique code that allows for the tracking of the report; the Reporter is responsible for recording and retaining this code.

2.2.1.1 SUPPLEMENTARY FORECASTS FOR ITALIAN SUBSIDIARIES

Owner: **Head of Breach Reporting System and/or Supervisory Body of the Subsidiary**

Employees and contractors of the Italian Subsidiaries have access to the online platform for reporting violations and report such violations to the Head of the Violation Reporting System, namely the Parent Company's Supervisory Board, which handles them.

A specific outsourcing agreement is in place between the Italian Subsidiaries and the Parent Company for the management of reports.

Where the Supervisory Board of the Italian Subsidiaries receives outside the electronic channel to the Parent Company's SB, a report that qualifies as whistleblowing in paper format (e.g., letter or registered mail) or digital format (e.g., email or certified email), they shall immediately communicate the report to the Parent Company's SB, which shall record the report on the platform and manage it.

If the report is potentially relevant for the purposes of Legislative Decree No. 231/2001, the Subsidiary's Supervisory Body will participate in both the preliminary assessment phase and the investigation, as well as in the conclusion of the investigation to assess the potential effects on the Subsidiary's 231 Compliance Program.

When the report concerns matters other than those governed by Legislative Decree No. 231/2001, the Subsidiary's Supervisory Body will receive, in addition to the initial notification of the report, a copy of the final summary report. Nevertheless, it may also be involved in the investigation if deemed appropriate by the Parent Company's Supervisory Body.

2.2.2 ANALYSIS OF THE REPORT

Owner: **Head of Breach Reporting System**

2.2.2.1 RECEIPT OF THE REPORT AND PRELIMINARY ANALYSIS

The Head of Breach Reporting System notifies the Reporter that the report has been acknowledged **within 7 (seven) days** of receipt.

The Manager then reviews the report and verifies the completeness of the information provided. If necessary, the Manager requests clarification from the Whistleblower and/or any other parties involved in the report, taking the necessary precautions required by law.

The Head of Breach Reporting System initiates **a preliminary analysis** in order to:

- assess the admissibility of the report based on:
  - its relevance to the scope of application of this procedure;
  - submission by one of the parties authorized to file reports;
  - the presence of the elements necessary to proceed with the analysis (see paragraphs 1.5 and 1.7, which specify the elements that must characterize a report);
- **classify the type of report,** with particular reference to its relevance or lack thereof for the purposes of Legislative Decree No. 231/2001 and for the purposes of the Anti-Corrupti.

The assessment of admissibility is conducted in accordance with the provisions of this procedure.

The Head of Breach Reporting System retains the right to request additional supporting information from the Reporter—where necessary—to support the report.

Following the preliminary analysis:

- if the report is deemed **inadmissible,** the Head of Breach Reporting System closes the report and informs the Reporter **within 3 (three) months** from the date of receipt or, in the absence of such notice, within three months from the expiration of the 7 (seven) day period following the submission of the report;
- if, on the other hand, it is deemed **admissible,** the Head of Breach Reporting System proceeds to the subsequent investigative phase.

Please note that the 3 (**three) month** deadline is not mandatory and that any feedback within that period may be merely preliminary.

2.2.2.2 PRELIMINARY INVESTIGATION

Owner: **Head of Breach Reporting System**

The investigation of admissible reports may involve different parties depending on the subject matter of the reports.

In particular, the **Head of Breach Reporting System**:

- **directly conducts the preliminary investigation** when the report concerns unlawful conduct that may be relevant under Legislative Decree No. 231/2001 and/or potential breaches of the MOG 231 and/or the BFF Banking Group Code of Ethics, which do not fall within the categories of reports of breaches of European regulatory provisions (e.g., offenses falling within the scope of application of European Union acts, acts or omissions that harm the financial interests of the Union, or acts or omissions concerning the internal market, as referred to in Article 26, paragraph 2, of the Treaty on the Functioning of the European Union)[4] . Depending on the specific subject matter of the report, the **Head of Breach Reporting System** is supported in conducting the investigation by **personnel from the relevant departments of the Bank and/or its Subsidiaries**, through the **Head of Internal Audit Department**: for example, if the report concerns potentially corrupt acts, the investigation is supported by **the Anti-Corruption Officer**, who is the Head of Compliance & AML Function;
- instructs the Head of Internal Audit Function to conduct the investigation when the report:
    - relates to unlawful conduct other than that covered by Legislative Decree No. 231/2001 and/or potential breaches of the 231 Compliance Model and/or the BFF Banking Group Code of Ethics, and/or when the report specifically concerns breaches of the aforementioned European regulatory provisions;
    - relates to breaches of specific sector regulations pursuant to Article 52-bis of Legislative Decree No. 385/1993, Article 48 of Legislative Decree No. 231/2007, and Article 4-undecies of Legislative Decree No. 58/1998.

In the cases in question, the **Head of Internal Audit Function**:

- is supported in the investigation by **personnel from the relevant functions of the Bank and/or its Subsidiaries**, depending on the specific subject matter of the report;
- keeps the Head of Breach Reporting System informed of developments in the investigation, including so that any necessary additions can be evaluated in a timely manner.

[4] See Art. 2, para. 1, letter a), items 3), 4), 5), 6) of Legislative Decree No. 24/2023.

The Head of Breach Reporting System and his support team may, in particular:

- conduct interviews with any internal/external parties, etc.
- engage external parties[5] to conduct the preliminary investigation or specific technical assessments (e.g., accounting or ICT).

The preliminary investigation must always be properly documented and archived to demonstrate due diligence in following up on the report.

The objective of the investigation phase is to conduct specific verifications, analyses, and assessments regarding the validity of the reported facts, including to formulate any recommendations regarding the adoption of necessary corrective actions in the affected business areas and processes with a view to strengthening the internal control system.

The Head of Breach Reporting System is not responsible for assessing individual liability, and the application of any disciplinary measures is always the responsibility of the Head of Human Resources & Organizational Development Department (see section 2.2.3 for further details).

2.2.2.3 FINAL REPORT AND FEEDBACK TO THE REPORTER

Owner: **Head of Breach Reporting System**

Once the preliminary investigation phase is concluded, the **Head of Breach Reporting System**:

- **In the event of an irrelevant report**—that is, if there is insufficient evidence to form an opinion regarding the reported matter or if the report is found to be unfounded—the Committee shall close the case with a reasoned decision and provide feedback to the Whistleblower;
- **in the event of a relevant report**, drafts a final summary report outlining the course of the investigation, the evidence gathered, and the conclusions reached, and provides feedback to the Whistleblower;

In both of the above cases, the Head of Breach Reporting System responds to the report **within 3 (three) months of the date of the acknowledgment of receipt or, in the absence of such acknowledgment,**

[5] In the event of the involvement of external parties, the duties of confidentiality and privacy provided for by Legislative Decree No. 24/2023 must also be extended to such external parties through specific contractual clauses to be included in the agreements entered into with the external party. Furthermore, the necessary designations regarding privacy must also be ensured.

within 3 (three) months of the expiration of the 7 (seven) day period following the submission of the report.

The Head of Breach Reporting System shall also provide feedback on the report within the aforementioned timeframes even **if the preliminary investigation has not been completed,** informing the Whistleblower of the activities carried out to date and/or the activities the Head intends to carry out.

In the latter case, the Head of Breach Reporting System will also notify the Reporter of the final outcome of the investigation into the report (dismissal or confirmation of the report's validity with referral to the competent Corporate Bodies).

>> Control C2: Monitoring of Report Handling Deadlines <<

The Whistleblowing Platform – Unione Fiduciaria automatically sends the Head of Breach Reporting System reminder emails with the deadlines by which the report must be processed. The Head of Breach Reporting System is responsible for tracking the processing stages within the application and making them available in the event of requests from the competent authorities, as required by current legislation.

2.2.2.4 EXTERNAL REPORTING AND PUBLIC DISCLOSURE

External Reporting

As an alternative to internal reporting, the Reporting Person may submit an **external report** through the channel available at or **the National Anti-Corruption Authority** (ANAC) if, at the time of submission, one of the following conditions applies:

- the Whistleblower has already filed an internal reporting and it has not been addressed or has not received a feedback within the timeframes set forth in Legislative Decree No. 24/2023[6] ;
- the Whistleblower has reasonable grounds to believe that if they were to file an internal reporting, it would not be effectively followed up or that filing such a report could result in the risk of retaliation;
- The whistleblower has reasonable grounds to believe that the breach may pose an imminent or clear danger to the public interest.

[6] The Head of Breach Reporting System shall provide the Whistleblower with feedback to the report within 3 months of the acknowledgment of receipt, issued within 7 days of the report being filed. In the absence of such acknowledgment, the feedback must be provided within 3 months of the expiration of the 7-day period following the submission of the report.

In addition, the Whistleblower may contact ANAC to report any retaliatory actions suffered. External reports are received by ANAC through the designated channels: online platform, verbal reports, and in-person meetings scheduled within a reasonable timeframe. For more information on the subject of the report and the procedures for filing an external report, please refer to the guidelines provided by ANAC on its official website.

This is without prejudice to the possibility of reporting breaches of banking and financial regulations:

- to **the Bank of Italy** pursuant to Article 52-bis, paragraph 2, of Legislative Decree No. 385/1993 and Article 48, paragraph 2, of Legislative Decree No. 231/2007;
- to **Consob** pursuant to Article 4-duodecies of Legislative Decree No. 58/1998 and Regulation (EU) No. 596/2014 on market abuse.

For **the Group's Subsidiaries and foreign Branches,** the external report may be submitted as indicated in Annex 1.

Public Disclosure

The Whistleblower may also choose to make a **public disclosure**, making information on the breaches available to the public through the press or media or otherwise through means of dissemination capable of reaching a large number of people.
Public disclosure of breaches must comply with the conditions set forth in Legislative Decree No. 24/2023 so that the Whistleblower may benefit from the protections provided, specifically:

- no feedback has been provided to an internal and/or external report within the time limits established by Legislative Decree No. 24/2023[7];
- there is reasonable cause to believe that the breach may constitute an imminent or obvious danger to the public interest;
- there are reasonable grounds to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as those in which evidence may be concealed or destroyed, or in which there is a well-founded fear that the recipient of the report may be colluding with the perpetrator of the breach or involved in the breach itself.

[7] In the case of external reports, ANAC shall provide feedback to the Whistleblower within 3 months or, if there are justified and substantiated reasons, within 6 months from the date of the acknowledgment of receipt of the external report or, in the absence of such acknowledgment, from the expiration of the 7-day period following receipt of the report.

2.2.3 OUTCOME OF THE INVESTIGATION

Owner: **Head of Breach Reporting System**

Once the final report has been drafted and the Whistleblower has been informed based on the findings of the investigation, the **Head of Breach Reporting System** may forward the report:

- to the Head of Group Human Resources & Organizational Development for the initiation of disciplinary proceedings
- as well as to other corporate functions of the Bank, and to the branches/subsidiaries affected by the facts described in the report, regarding any necessary measures to bring the 231 Compliance Management System and corporate procedures into compliance, while always maintaining the confidentiality obligations required by law.

However, the Head of Breach Reporting System, in the event that the report concerns matters involving the Bank or a Subsidiary, relating to:

- a **Corporate Body**, with the exception of the Chairman of the Board of Directors, the Chief Executive Officer, the General Manager, and the Board of Auditors, or a **Senior Executives,** the Head of the Whistleblowing System shall send the report to the Chairman of the Board of Directors of the Parent Company, the Chief Executive Officer and General Manager of the Parent Company (GCEO), and the Board of Statutory Auditors of the Parent Company;
- the **Chairman of the Board of Directors or any member of the Board of Directors**, the Head of Breach Reporting System will send the report to the Board of Auditors;
- **the Chief Executive Officer and General Manager**, the Head of Breach Reporting System will send the report to the Chairman of the Board of Directors of the Parent Company and to the Board of Auditors;
- the **Board of Auditors or any of its members**, the Head will forward the report to the Chairman of the Board of Directors, the Chief Executive Officer, and the General Manager.

If the report concerns **situations of particular significance and gravity** (regardless of the status of the reported parties indicated above), the Head of Breach Reporting System shall promptly inform the relevant s and Corporate Bodies of the Bank or its Subsidiaries, proposing the adoption of the most appropriate actions.

In accordance with the principle of confidentiality regarding the identity of the Whistleblower and the information gathered during the various stages of report handling, **the shared report will be anonymized** and will contain only the information necessary to understand the subject of the report.

2.2.4 DOCUMENT RETENTION

Owner: **Head of Breach Reporting System**

The Head of Breach Reporting System retains relevant documentation pertaining to the report including, but not limited to, collected evidence, analysis documents, and final assessment reports for a period not exceeding 5 (five) years. Documentation is stored directly on the Whistleblowing platform and/or on network drives (in the latter case, files will be password-protected). The documentation in question is considered confidential and therefore accessible only to authorized persons.

Reports (written and oral) and the related documentation must be retained by the Head of Breach Reporting System for the time necessary to process the reports and, in any case, for **no longer than 5 (five) years** from the date of notification of the final outcome of the reporting procedure.

At the end of the 5 (five) year retention period, the **paper documents** relating to the reports received must be **destroyed** in such a way as to render the information they contain illegible.

>> Control C3: Data Retention Control <<

Once a year, the Head of Breach Reporting System verifies that the archived documentation consists solely of that pertaining to the retention period required by law and, where necessary, deletes the reports.

2.2.5 ANNUAL REPORTING TO THE GROUP'S BOARD OF DIRECTORS AND REPORT REGISTER

Owner: **Board of Directors, Head of Whistleblowing System**

The Head of Breach Reporting System reports **annually on** the proper functioning of the internal reporting system, providing in a dedicated report aggregate information (including archived reports) while ensuring the confidentiality and anonymity of the personal identities involved, the activities carried out, and the follow-up given to relevant reports received.

The annual report will provide information on the most significant data, including:

- number of reports handled;
- classification of the reports handled;
- disciplinary sanctions imposed;
- reports filed with a description of the reason;
- major process gaps identified;
- corrective actions in progress and completed.

In drafting the report, the Head of Breach Reporting System is required to comply with the provisions of the regulations on the protection of personal data.

This report is submitted for approval to the Bank's Board of Directors and made available to Group staff in the repository dedicated to internal regulations. For reports concerning Subsidiaries, this report is sent to their respective Boards of Directors.

The Head of Breach Reporting System maintains a specific register of reports, managed electronically as part of the IT procedure. Data from the register may be extracted by the Head of Breach Reporting System upon specific requests from supervisory and/or judicial authorities, while ensuring privacy safeguards in the event that personal data is present within the register.

3 RISKS AND CONTROLS TABLE

Process	**2.1 – TRAINING AND AWARENESS**	
Activities	**2.1.1 Employee training during onboarding and ongoing training**	
Risk	**RISK/R1/Operational/**	Risk of Training Non-Completion Impact: > **Low <** Frequency**: > Low <** Gross Risk: **> Low <**
Control	**Control C1: Verification of training completion** **Head of Unit: GHR & OD Department** Effectiveness: > **Medium-High <**	

	Frequency: **> Low <** Net Risk: **> Low <**	
Process	**2.2 MANAGEMENT OF REPORTS**	
Activities	**2.2.2 Analysis of the report**	
Risk	**RISK/R1/Operational/**	Risk: Monitoring of Deadlines Impact: > **Medium-Low <** Frequency: **> Medium-Low <** Gross Risk: **> Medium-Low <**
Control	**CONTROL C2: Monitoring of Report Handling Deadlines** **Head of Unit: Manager of the Breach Reporting System** Effectiveness: > **High <** Frequency: **> Low <** Net Risk: **> Low <**	
Risk	**RISK/R1/Operational/**	Risk: Monitoring of Deadlines Impact: > **Medium-Low <** Frequency: **> Medium-Low <** Gross Risk: **> Medium-Low <**
Control	**CONTROL C3: Verification of data archiving** **Head of Unit: Manager of the Breach Reporting System** Effectiveness: > **High <** Frequency: **> Low <** Net Risk: **> Low <**	

4 ATTACHMENTS

ATTACHMENT 1 - Internal Reporting

NATION	INTERNAL REPORTING	RELEVANT REGULATIONS
Spain	• The Spanish Law "on the protection of persons reporting regulatory breaches and the fight against corruption" guarantees Whistleblowers protection against retaliation only if their reports fall within the scope of the law, as follows: - actions or omissions that may constitute a criminal offence or a serious or very serious administrative infringement. - any actions or omissions that may constitute infringements of European Union law, provided that they; ○ fall within the scope of the EU acts listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law; ○ affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); ○ have an impact on the internal market as referred to in Article 26(2) TFEU, including infringements of EU competition and state aid rules or corporate tax rules. • The Spanish Law "on the protection of persons reporting regulatory breaches and the fight against corruption" shall not apply to information regarding violations in the conduct of **procurement procedures** that contains classified information or that has been designated as secret or confidential, or to those whose implementation must be accompanied by special security measures in accordance with applicable law, or where the protection of interests essential to national security so requires. • The **Independent Authority for the Protection of Whistleblowers** (an independent Spanish public body responsible for the nationwide enforcement of the Whistleblower Protection Act to ensure the protection of Whistleblowers, combat corruption, and coordinate with other similar public bodies) has	Spanish Law No. 2/2023 of February 20, 2023, on the protection of persons reporting regulatory breaches and the fight against corruption. Recommendation No. 1/2026 of the Independent Authority for the Protection of Whistleblowers regarding the design and implementation of an internal reporting system, published on January 14, 2026.

	published Recommendation 1/2026, which reiterates the obligation to designate a "Head of Breach Reporting" and notify the Independent Authority for the Protection of Whistleblowers by April 10, 2026.This individual may also be a collegial body, but an internal representative must be designated. • BFF Bank S.p.A. has notified the Independent Authority for the Protection of Whistleblowers that the "Head of Breach Reporting" is the Parent Company's Supervisory Body and has designated the **Head of Internal Audit Function** as its representative. BFF Bank S.p.A. will notify the Authority of any changes. • At the Whistleblower's request, an oral report may be made during an **in-person meeting,** which the organization shall schedule within **7 (seven) days** of receiving the request. • **Oral reports**, including those conducted during in-person meetings that may be requested by the whistleblower, must be documented in one of the following ways, subject to the whistleblower's prior consent: a) by recording the conversation in a secure, durable, and accessible format, or b) through a complete and accurate transcript of the conversation. • The protection afforded to Whistleblowers who have made a public disclosure is granted on the same terms as those applicable to other forms of reporting, except in cases where the information has been disclosed directly to the press. • **Protection against retaliation**, must be extended up to at least **2 (two) years** after the end of the investigations. • The procedure for handling reports must expressly safeguard the rights of the person concerned. **The person concerned has the right to be informed** of the acts or omissions attributed to them and to be heard at any stage of the proceedings. Furthermore, the presumption of innocence of the person concerned is upheld throughout the entire process. • When the reported facts may be indicative of a criminal offense, the Company must immediately refer the reported information to the Public Prosecutor's Office, or to the European Public Prosecutor's Office where the facts affect the financial interests of the European Union.	

	• The Spanish Law "on the protection of persons reporting regulatory breaches and the fight against corruption" establishes the following **sanctions for the Bank**: (i) fines of up to EUR 100,000 for minor infringements; (ii) fines ranging from EUR 100,001 to EUR 600,000 for serious infringements; and (iii) fines ranging from EUR 600,001 to EUR 1,000,000 for very serious infringements. In addition, in the case of very serious infringements, the competent authority may impose supplementary measures, including public reprimand, a prohibition on obtaining public subsidies or tax benefits for a maximum period of four years, and a prohibition on contracting with the public sector for a maximum period of three years. • The Spanish Law "on the protection of persons reporting regulatory breaches and the fight against corruption" also cover **sanctions for individual persons involved in any potential infringement**, which include: (i) fines ranging from EUR 1,001 to EUR 10,000 for minor infringements; (ii) fines ranging from EUR 10,001 and EUR 30,000 for serious infringements; and (iii) fines ranging from EUR 30,001 and EUR 300,000 for very serious infringements.	
Portugal	• The internal reporting channel must be structured in such a way as to allow reports to be submitted anonymously or with identification of the Whistleblower, in writing and/or oral , including through **electronic authentication** tools, such as electronic ID cards, mobile digital keys, as well as any other electronic identification system recognized and issued by European Union member states. The internal reporting channel must also enable reporting by telephone or through another voice messaging system and, at the Whistleblower's request, in a **face-to-face meeting**. • The same channel must also include a **mandatory system for managing and following up** on reports, capable of ensuring an adequate **feedback to the Whistleblower**. In particular, upon the Whistleblower's request, information regarding the outcome of the verifications, analyses, and investigation must be provided **within 15 days from the date of the request** or, if the investigation concludes later, within 15 days of its conclusion.	Portuguese Law No. 93/2021 of December 20, 2021, on the general regime for the protection of Whistleblowers.
Poland	• At the Whistleblower's request, an oral report may be made during an **in-person meeting**, which the organization shall schedule **within 14 days** of receiving the request.	Polish Law No. 928/2024 of June 14, 2024, on the

	• Personal data and other information contained in **the internal reporting register** must be **retained for a period of 3 years** from the completion of the proceedings.	protection of Whistleblowers.
Greece	• Greek law designates the **Y.P.P.A. (Υπεύθυνος Παραλαβής και Παρακολούθησης Αναφορών)**, or the **Officer Responsible for Receiving and Monitoring Reports**, as the responsible party; this is a highly specialized, independent individual with appropriate professional expertise. • The internal report is submitted in writing or orally or via an IT platform. • Internal reporting channels are designed to: - ensure the confidentiality of the whistleblower's identity; - ensure that the channel is accessible to all individuals authorized to submit a report. • Confirmation of receipt of the information must be provided within **7 days**. • Feedback on the report is provided within **3 months** of receipt where the complexity of the case so requires, this deadline may be extended up to a maximum of **6 months**. • The internal procedure must provide clear information about the Reporting process, communication to the External authorities and the Protection framework. • The internal reporting channel, accessible to persons with disabilities, must enable reporting by telephone or through another voice messaging system. At the **request of the Whistleblower**, the opportunity to hold a **direct meeting** is guaranteed; the organization will schedule this meeting within. with the Y.P.P.A. (officer in charge of receiving whistleblowing reports) **within a reasonable period of time.**	Greek Law No. 4990/2022 of November 15, 2022, on the protection of persons reporting breaches of EU law.
Czech Republic	• **Reports** may concern not only alleged breaches of European Union regulations falling within their respective scopes of application, cases that meet the criteria for a criminal offense but also conduct that exhibits signs of potential illegality, even if not yet established, provided that it is theoretically capable of giving rise to the **imposition of an administrative fine of up to 100,000 CZK** (equivalent to approximately 4,079 euros) and in other situations specified by law. • The Whistleblowing internal channel is managed by BFF Bank S.p.A., Parent Company of the Group.	Act No. 171/2023 of the Czech Republic of June 15, 2023, on the Protection of Whistleblowers.

	• The internal reporting channel must be **managed by specifically designated and qualified individuals ("Relevant Person"),** who possess adequate professional expertise, operational independence, and decision-making autonomy in carrying out the activities of receiving, analyzing, and following up on reports. Such systems may **not** be managed **by departments, offices, or organizational units** as a whole, in order to ensure a high level of confidentiality, impartiality, and effectiveness in the report management process. • At **the Whistleblower's request**, the opportunity to **meet directly** with the person responsible for handling the report is guaranteed. Such a meeting must be arranged in compliance with appropriate measures to protect the confidentiality of the information and the Whistleblower's identity. • People who report, file a complaint, or make a public disclosure shall not incur any civil, criminal or administrative liability for such disclosure, provided that they had reasonable grounds to believe that the report was necessary to identify unlawful conduct within the meaning of Article 2(1)(1). Such disclosure shall not be considered a breach of banking secrecy, of any contractual duty of confidentiality, or of any statutory duty of confidentiality, including those under the Tax Code or other laws governing employment or similar activities. The **protection does not apply**, when the disclosure concerns: i) the protection of information whose disclosure could clearly compromise ongoing criminal proceedings, or the protection of specific facts under the law governing crisis management; ii) in connection with the provision of legal assistance in proceedings before a court or other public authority. • A **feedback** to the report is provided **within 30 days** of the date of receipt. If the **complexity of the case** makes it necessary, this deadline may be **extended** for subsequent periods of **30 days** each, up to a maximum of **two extensions**. In any case, the total time limit for handling and responding to the report may not exceed 90 days. The Relevant Person is obliged to notify the Whistleblower in writing of the extension of the deadline and the reasons for its extension before its expiry. • The subsidiary publishes the name of the head of Breach Reporting system and the relevant person	

Slovak Republic	• The Slovak Republic, pursuant to Act No. 54/2019, regulates **two types of reports**: - **Whistleblowing report**: a communication made by a person who reports facts, acts, or conduct of which they have become aware in the course of their employment or professional relationship and which are harmful, irregular, or otherwise detrimental to the company; - **Qualified Whistleblowing Report:** a report which, due to the content and concrete utility of the information provided, contributes or may contribute to the investigation of conduct that is particularly serious and harmful to the company. Given its significance, such a report is considered of particular importance and entails the application of enhanced protection measures provided for by current legislation in favor of the Whistleblower. • Personal data and additional information contained in **the internal reporting register** are **retained for a period of 3 years** from the date of receipt of the report, in compliance with applicable data protection laws and limited to the time necessary to pursue the purposes related to the management and any investigation of the reports. • At the **Whistleblower's request,** the opportunity to hold a direct meeting is guaranteed; the organization will schedule this meeting within a reasonable timeframe after receiving the request. • The **Whistleblower** has the right to request a **review of the decision to dismiss or reject** the report within **15 days** of being notified of the decision. • A **feedback** must be provide to the Whistleblower **within 90 days** of acknowledging receipt.	Act of the Slovak Republic No. 54/2019 of September 1, 2023, on the Protection of Whistleblowers.

External Reporting

COUNTRY	AUTHORITY	RELEVANT LEGISLATION
Spain	• Madrid Municipal Office Against Fraud and Corruption (specifically for corruption offenses); • Bank of Spain (in the case of BFF Bank S.p.A. Branch in Spain); • Independent Authority for the Protection of Whistleblowers, A.A.I. (AIPI). • **The Independent Whistleblower Protection Authority (AIPI)** ensures that the Whistleblower is informed of the decisions made regarding the report. Specifically, **within 5 days** of the date the	Spanish Law No. 2/2023 of February 20, 2023, on the protection of persons reporting regulatory breaches and on the fight against corruption. Recommendation No. 1/2026 of the Independent Authority for the Protection

	decision is made, the AIPI notifies the Whistleblower of whether the report has been deemed admissible or inadmissible. This notification requirement does not apply if the report was submitted anonymously or if the Whistleblower has expressly waived the right to receive notifications. • The Spanish Law "on the protection of persons reporting regulatory breaches and the fight against corruption" the internal reporting system designated as the preferred channel; however, this preference must not limit or preclude the reporter's right to file an external report at any time.	of Whistleblowers regarding the design and implementation of an internal reporting system, published on January 14, 2026.
Portugal	• Public Prosecutor's Office; • Criminal police agencies; • Bank of Portugal; • Independent administrative authorities; • Public institutes; • **The general inspectorates** and **equivalent entities and other central services** of the direct administration of the State endowed with administrative autonomy; • Local authorities; • Public associations; • National Anti-Corruption Mechanism and the Public Prosecutor's Office.	Portuguese Law No. 93/2021 of December 20, 2021, on the general regime for the protection of Whistleblowers.
Poland	• Ombudsman and public authorities • **The Ombudsman** receives external reports but intervenes directly only in cases involving *"constitutional freedoms and human and civil rights"* arising in relations between citizens and public authorities. • For all other reports (listed in Article 3, Part 1, points 1 through 16 of the document **"The Protection of Whistleblowers")**, the Ombudsman conducts a preliminary analysis and forwards them to the competent public authority **within 14 days,** informing the Whistleblower that the report has been forwarded **to the competent public authority** or, if the Ombudsman refrains from forwarding the report.	Polish Law No. 928/2024 of June 14, 2024, on the Protection of Whistleblowers.
Greece	• National Transparency Authority (E.A.D. - Εθνική Αρχή Διαφάνειας) • The report to the "National Transparency Authority" is submitted in writing or orally or via an electronic platform, accessible to persons with disabilities. • The oral report may be submitted via telephone or other voice messaging systems, as well as through a personal meeting with a person designated by the	Greek Law No. 4990/2022 of November 15, 2022, on the protection of persons reporting breaches of EU law.

	N.T.A. within a reasonable time, **upon request of the informant.**	
Czech Republic	• Ministry of Justice • Labor Inspection Authority • Public disclosure can be done when: - the whistelblower submitted a report through the internal reporting system and to the Ministry or only to the Ministry and no appropriate action was taken within the time limits set out in the Law, in particular the competent person did not assess the justification of the notification, the obliged entity did not take another appropriate measure to prevent or remedy the unlawful situation, or the civil servant did not assess the notification; - the whistelblower has reasonable grounds to believe that the infringement referred to in the report may lead to an immediate or manifest threat to internal order or security, life or health, the environment or any other public interest, or to irreparable harm, or; - the whistelblower has reasonable grounds to believe that, in the event of a notification to the Ministry, there is an increased risk that he or the person referred to in Section 4(2)(a) to (h) od the Law will be subject to retaliation or that the procedure under Title III is jeopardised, in the event of a notification to the Ministry.	Czech Republic Act No. 171/2023 of June 15, 2023, on the protection of Whistleblowers.
Slovak Republic	• Whistleblower Protection Office (WPO). • **Public prosecutor's office**, or **administrative authority competent** to conduct proceedings regarding an administrative offense that constitutes a serious anti-social act pursuant. • Relevant institution, body, office, or agency of the European Union. • Slovak law grants Whistleblowers of serious anti-social activity: - the right to protection directly from the Whistleblower Protection Office (WPO) or the prosecutor; - an employee's right to request that **the Anti-Corruption Office** to suspend the effect of an employment-related action if they believe it constitutes an act of retaliation.	Act of the Slovak Republic No. 54/2019 of September 1, 2023, on the Protection of Whistleblowers.