Whistleblowing Policy

Code	Version	Date of approval	Date of entry into effect
PY071	001	22/06/2023	01/07/2023

CONTENTS

VERSIONING			
Version	**Date of approval**	**Summary description of amendments**	**Repealed/Replaced regulation**
001	22/06/2023	- *This Policy governs the organisational and procedural aspects of the internal whistleblowing systems*	*Whistleblowing Procedure*

POLICY OWNER
Head of **Compliance and Anti-Financial Crime Department**

GLOSSARY	
Banca Generali or Bank or Company or Parent Company	Banca Generali S.p.A.
Corporate Governance Code	The Corporate Governance Code approved by the Corporate Governance Committee and promoted by Borsa Italiana S.p.A.
Subsidiaries	The companies controlled from time to time by Banca Generali and belonging to the Banca Generali Group
Subsidiaries of the Banking Group	The banking, financial and instrumental companies — with registered office in Italy and abroad — controlled from time to time by the Company and belonging to the Banking Group
Legislative Decree No. 24/23	Italian Legislative Decree No. 24 of 10 March 2023 implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and concerning provisions on the protection of persons who report breaches of Italian national law
Supervisory Provisions	*Supervisory Provisions for Banks* adopted through Bank of Italy Circular No. 285 dated 17 December 2013, as subsequently amended and extended
Banca Generali Banking Group or Banking Group	The group made up of the banking, financial and instrumental companies — with registered office in Italy and abroad — controlled from time to time by the Company and of which Banca Generali is the Parent Company
Banca Generali Group or Group	The group made up of the companies associated with each other by virtue of the control exercised by Banca Generali
Generali Group	The corporate group of which Assicurazioni Generali S.p.A. is the Parent Company and made up of the latter and the companies controlled by it pursuant to Article 2359, paragraphs 1 and 2, of the Italian Civil Code
Head of Internal Whistleblowing Systems or Head of Whistleblowing	Head of the Compliance and Anti-Financial Crime Department
Reporting persons/ Whistleblowers or Beneficiaries of the whistleblowing system	Individuals as defined in point 4.1. who work for or have a relationship with the Bank or the Banking Group and who are entitled to report information pursuant to applicable laws and this Policy

Concern	Knowledge of or reasonable suspicion on practice or conduct considered, in good faith, to be inappropriate or incompatible with the law and/or internal policies and procedures.
Breaches	Conduct, acts or omissions that harm to the public interest or to Banca Generali's integrity. They include the offences, acts, behaviour and conduct described in greater detail in Article 2, paragraph 1, of Italian Legislative Decree No. 24/23
Public Disclosure	A situation in which a person makes information on breaches available in the public domain using printed or electronic supports or, in any case, through communication means able to reach a large number of people
Facilitator	A natural person who assists a reporting person in the reporting process and operates in a work-related context, and whose assistance should be confidential
Retaliation	Any behaviour, act or omission — including where attempted or threatened — that is undertaken in view of a report, a complaint with a judicial or accounting authority or public disclosure and that causes or may cause the person who made the report or complaint unjust harm, directly or indirectly.

1. INTRODUCTION

European and Italian lawmakers have introduced whistleblowing systems (the term comes from 'whistle blowers' used in the past to refer to police officers who blew whistles to try to stop wrongdoing).

Whistleblowing systems are set up to enable the reporting of breaches of rules of which a person becomes aware in a work-related context in order to facilitate the spread of ethically compliant conduct and safeguard the rule of law.

The applicable regulatory framework governs the organisational and procedural aspects of the internal whistleblowing systems that banks must adopt to allow the internal reporting of acts or facts that could represent a breach of banking laws. Such provisions are based on two main principles:

- protection of the whistleblower and other parties against retaliatory or discriminatory behaviour or other unfair consequences of reporting;
- the guarantee of confidentiality of the personal data of the whistleblower and of the party presumed responsible for the breach, without prejudice to the rules governing investigations or proceedings initiated by the judicial authority with regard to the circumstances reported.

1.1. SUBJECT MATTER AND OBJECTIVES OF THIS POLICY

In line with the principles that inspire the Generali Group, Banca Generali promotes and facilitates the spread of a company culture of rule of law characterised by ethical behaviour and ensures effective and efficient measures to preventing, managing and, where necessary, internally reporting any irregularities or breaches of the rules governing company activity, through secure, confidential channels. To this end, the Bank requires its Personnel, when performing their duties, to respect the highest standards of honesty and propriety, as well as to safeguard the resources for which each person is responsible.

Banca Generali adopts this Policy in order to set forth the criteria and rules that allow to manage any reports that its personnel may make, regarding frauds and suspicious behaviour, irregularities in business conduct or breaches of the rules governing its activity.

More specifically, this Policy aims to define:

- the bodies and functions involved in the management of reports, describing their roles and responsibilities;
- the channels available to the whistleblower to report any alleged anomaly or breach committed by employees, members of corporate bodies or third parties;
- the objective scope and content of the report;
- the whistleblowers (reporting persons) and the measures set forth to protect them;
- the procedures managing the report;
- the methods of communication to the whistleblower and the person concerned by the report of the state of progress of the assessment of the report;
- the procedures for record-keeping of documents.

In order to ensure its dissemination, this Policy is published on the Bank’s institutional website and on the Company's Intranet.

1.2. DOCUMENT MANAGEMENT

This Policy has been adopted through an approval resolution passed by the Bank's Board of Directors.

Any amendments to this Policy that are necessary and/or appropriate, classified as "of lesser importance" according to the *Guidance policy to prepare and update corporate policies and regulations*, are approved by the Chief Executive Officer on the proposal of the Owner (as defined below) and of the Organisation Department, in consultation, where needed, with the Corporate Affairs and Relations with Authorities Department.

The Compliance and Anti-Financial Crime Department (hereinafter, the "**Owner**") is responsible for verifying on an annual basis from the date of issue/last revision, the possible need for updating this Policy, taking into account its compliance with the relevant regulatory framework, the strategy of the Bank and the entire Group, and the operational and organisational context in which the Bank and the Group operate.

1.3. REGULATORY FRAMEWORK

External regulations

- Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- Italian Legislative Decree No. 24 of 10 March 2023 implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and concerning provisions on the protection of persons who report breaches of Italian national law;
- Consolidated Law on Banking (TUB) – Italian Legislative Decree No. 385 of 1 September 1993, as further amended and extended;
- Consolidated Law on Finance (TUF) – Italian Legislative Decree No. 58 of 24 February 1998, as further amended and extended;
- Private Insurance Code – Italian Legislative Decree No. 209 of 7 September 2005, as further amended and extended;
- Italian Legislative Decree No. 231 of 21 November 2007, as further amended and extended;
- Italian Legislative Decree No. 90 of 25 May 2017 implementing Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directives 2005/60/EC and 2006/70/EC and implementing Regulation (EU) No 2015/847 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006;
- Italian Legislative Decree No. 231 of 8 June 2001, as further amended and extended, governing administrative liability of legal entities, companies and associations, including with no legal personality;
- Italian Personal Data Protection Code – Legislative Decree No. 196 of 30 June 2003, as further amended and extended;
- Bank of Italy Circular "Supervisory Provisions for Banks" No. 285 of 17 December 2013, as further amended and extended;
- Corporate Governance Code for Listed Companies of Borsa Italiana.

Internal regulations

- Banca Generali's Internal Code of Conduct;
- Description of the Organisation and Management Model pursuant to Legislative Decree No. 231/2001;
- Banca Generali's Internal Fraud Policy;
- Italian National Collective Labour Agreement for the Credit sector (CCNL);
- Company's Disciplinary Regulations

1.4. SCOPE OF APPLICATION

This Policy applies to Banca Generali and the Subsidiaries of the Banking Group. The Subsidiaries implement the Policy in compliance with the legal and regulatory requirements applicable to their activity or place of incorporation. If any of the provisions contained in the Policy are less restrictive than local legislation, the company concerned will adopt the most restrictive local law in force.

The bodies with strategic oversight functions of the Subsidiaries of the Banking Group are required to adopt this Policy, by specific resolution, as adopted by the Parent Company, thereby assuming responsibility for ensuring knowledge thereof and application to matters within their scope and business, adapting it to their own organisational structure. If conflicts with local laws and regulations emerge, or if, in application of the proportionality principle, it becomes necessary to derogate from this Policy, the body with managing functions (e.g., Managing Director/General Manager) of the Group's company in question provides, in advance, an explicit, reasoned account of the necessary derogations to the Parent Company.

2. ROLES AND RESPONSIBILITIES

The Bank's main bodies and functions involved in the process governed by this Policy are:

Board of Directors: as the body with the strategic supervision function, the Board of Directors approves this Policy and any amendments of greater importance thereto; it also approves the annual report on the proper functioning of internal whistleblowing systems; and it is informed, along with the Chief Executive Officer and General Manager and the Board of Statutory Auditors, of breaches of particular severity;

Chief Executive Officer and General Manager: he approves, with the power to delegate, amendments of lesser importance to Policies, as defined in the Guidance policy to prepare and update corporate policies and regulations; he decides on measures within his purview to be taken against employees involved in breaches in accordance with the powers delegated by the Board of Directors;

Compliance and Anti-Financial Crime Department: the Head of the Department, who serves as *Head of Internal Whistleblowing Systems,* ensures the proper performance of the report-handling procedure, appropriate management of the whistleblowing system and the related process of reporting to company bodies;

Internal Audit Department: the Head of the Department collaborates with the *Head of Internal Whistleblowing Systems* in the ensuing assessment process and investigations; the Head of the Intrnal Audit Department is identified as the alternative recipient of reports in the cases indicated in the Policy;

Human Resources Department: it decides, for the matter under its purview, on the relevant measures to be taken against those responsible for breaches, as the structure responsible for enforcing disciplinary measures against employees in accordance with the powers delegated by the Board of Directors and/or the Chief Executive Officer and General Manager.

3. PRINCIPLES AND GUIDELINES

3.1. BENEFICIARIES OF THE WHISTLEBLOWING SYSTEM

Pursuant to the regulations in force, reports can be made by the following individuals who work for or have a relationship with the Bank or the Banking Group:

- employees (regardless of contract type), interns;
- Financial Advisors;
- third parties who have long-term relations and business relationships with the Bank or the Banking Group (e.g., coordinated and ongoing collaboration, consultants permanently within the company on the basis of time material contracts, etc.).
- suppliers of goods and service providers;
- individuals with administration, management, control, oversight or corporate representation functions;
- shareholders.

Reports are also allowed:

- when the legal relationship has not yet begun, if the information regarding the breaches was acquired during the selection process or in other precontractual phases (e.g., candidates);
- after the termination of the legal relationship, if the information regarding the breaches was acquired before the termination of the relationship (e.g., retirees).

3.2. FACTS THAT MAY BE REPORTED AND EXCLUSIONS

The internal whistleblowing systems are set up in order to allow whistleblowers (reporting persons) to report conduct, acts or omissions that harm to the public interest or to the integrity of Banca Generali or the Banking Group and that may represent, in particular:

- a breach of the rules governing banking and financial brokerage activities, as well as the distribution of insurance products;
- a potential or actual breach of the provisions designed to prevent money-laundering and terrorist financing;
- a serious irregularity or breach of the laws and regulations applicable to the Bank and the Banking Group, as specified below.

Reports should therefore concern negligent, unlawful, irregular or unfair conduct relating to work activities, for which there is reasonable suspicion or of which a person has become aware in the conduct of his or her functions, including, but not limited to:

- administrative, accounting and tax irregularities;
- irregularities concerning anti-money laundering and prevention of financing of terrorism;
- market-abuse irregularities and other irregularities relating to the provision of investment services and activities;
- irregularities relating to the distribution of insurance products;
- breaches of data confidentiality rules;

- breaches of the Internal Code of Conduct;
- breaches of the Organisational and Management Model pursuant to Legislative Decree No. 231/2001;
- violation of usury rules;
- bullying and harassment;
- corruption;
- misappropriation and embezzlement (regarding money and tangible and intangible goods);
- fraud;
- offences relating to bank lending operations (e.g., transparency, etc.);
- unlawful exercise of delegated powers;
- other irregularities that may constitute violations of banking laws.

The acts or circumstances that are excluded from the provisions of this Policy include, by way of example and without limitation:

- customers' requests;
- suspicious transactions pursuant to Legislative Decree No. 231/2007, as further amended and extended, for which the specific procedure envisaged by applicable legislation must be activated;
- information already in the public domain (e.g., newspaper articles, public audit reports, etc.);
- complaints of a personal nature by the whistleblower, claims/petitions that come under the rules governing the working relationship; or complaints regarding relations with hierarchical superiors or colleagues;
- immediate risks to life or property (in these cases, other procedures should be activated, including, but not limited to, the anti-fire plan and the business continuity plan, or the national emergency numbers should be called);
- unconfirmed rumours or hearsay.

Reports may involve:

- employees and executives, regardless of position and rank;
- members of corporate bodies;
- third parties linked to the above-mentioned individuals (suppliers, consultants).

3.3. PROCEDURES FOR REPORTING BREACHES

Without prejudice to the possibility of personnel to contact their direct supervisors/managers for any doubts or concerns, individuals (as defined in point **Errore. L'origine riferimento non è stata trovata.**. above) who identify acts or behaviours that, in good faith, they regard as in breach of the rules may submit a report using the following channels:

1. through the IT platform available from the corporate websites, by telephone or via the Web;
2. by e-mail to the dedicated address (segnalazioni.whistleblowing@bancagenerali.it);

3. sending a letter in a private and confidential envelope to the "*Responsabile della Direzione Compliance e Anti-Financial Crime (Head of the Compliance and Anti-Financial Crime Department)*";
4. requesting, sufficiently in advance, to meet the *Head of the Compliance and Anti-Financial Crime Department*.

The Head of the Compliance and Anti-Financial Crime Department and the Head of the Internal Audit Department (and their designated representatives) can access the dedicated IT platform.

It should be noted that this platform allows to specify whether the report involves the Compliance and Anti-Financial Crime Department or the Internal Audit Department, so that it can be assessed, with no conflicts of interest, by the Head of the Internal Audit Department or by the Head of the Compliance and Anti-Financial Crime Department, respectively.

In the event of a report made in writing in a private envelope, the *Head of Internal Whistleblowing Systems* is responsible for informing the Head of the Internal Audit Department of the report received.

Whistleblowers may decide to make an anonymous report. In this event, the dedicated IT platform provides an ID code to allow the exchange of information with the *Head of Internal Whistleblowing Systems*.

Although anonymous reports are accepted, the Banking Group encourages whistleblowers to reveal their identities when submitting a report, because this usually permits a more effective investigation. In order to facilitate disclosure of identity, the Banking Group has established specific protection measures against any retaliations.

The Whistleblower is also required to declare whether he or she has a private interest in the whistleblowing report.

Reports must be detailed, reasonable and significant and cannot be based on a prejudice or preconception.

They should contain the details needed to permit an investigation. Reports without sufficient information cannot give rise to an investigation and therefore must be inquired into in collaboration with the whistleblower in order to gather sufficient information to initiate an investigation.

Whistleblowers are required to collect and organise the relevant information in order to facilitate the internal investigation, providing a clear, sufficient picture to support an understanding of the case and enable an impartial, fair investigation by the competent function.

3.4. COMPILING THE REPORT

Below are some instructions for properly compiling reports, valid regardless of the channels elected by the whistleblower, particularly in cases not involving the use of the dedicated IT platform, which entails compilation of a specific form.

The report should include at least the following information:

1. Company and corporate structure referred to in the report;
2. any private interest in the report;
3. type of breach;
4. description of the facts reported;
5. date or period in which the facts reported occurred;

6. how the whistleblower became aware of the facts reported;
7. corporate personnel and functions involved in the facts reported.

The report may also include the following information, useful for investigation purposes:

8. any beneficiaries of the reported events;
9. any parties harmed by the reported events;
10. any economic value of the facts reported;
11. any third party involved in the facts reported (suppliers, customers, etc.);
12. any information useful to assess the truthfulness of the report;
13. any other useful information.

The report may also be accompanied by supporting documentation.

3.5. EXAMINATION AND PRELIMINARY ASSESSMENT OF REPORTS

The *Head of Internal Whistleblowing Systems* carries out a preliminary assessment to ensure appropriate management of the case as follows:

1. ensures that there are no conflicts of interest and that the question falls within his or her purview and, if it does not, sends the report directly to the competent body;
2. issues a written acknowledgement of receipt of the report within seven days of its receipt;
3. verifies that the report is sufficiently detailed to proceed with the assessment;
4. where the information is not sufficient, he or she asks the Whistleblower to provide additional information, without there being an obligation to provide such information;
5. if the report is not sufficiently detailed and additional information has not been received, he or she closes the report and informs the Whistleblower;
6. if the report is sufficiently detailed, he or she proceeds with the investigation.

The same procedure is applied by the Head of the Internal Audit Department when he or she is required to manage a report as an alternative channel to the Head of the Compliance and Anti-Financial Crime Department, in the cases provided for by this Policy.

3.6. INVESTIGATIONS AND COMMUNICATION OF OUTCOME

Once the preliminary assessment is completed, the *Head of Internal Whistleblowing Systems* initiates investigations into the case.
Investigations must have a reasonable duration and are carried out by the Compliance and Anti-Financial Crime Department and/or the Internal Audit Department according to the type of report and the respective areas of competence. These Departments shall operate independently and according to their approaches and standard aims, and may avail themselves of the support of corporate structures and/or technical advisors (e.g., external law firms or specialists internal to the Bank) regarding subjects that do not fall within their specific remittance.

For reports related to presumed breaches of anti-money laundering legislation, the Head of Anti-Money Laundering Function will be responsible for the appropriate assessments and, where

necessary, for submitting any communications envisaged by Legislative Decree No. 231 of 21 November 2007, as further amended and extended.

In such cases, the *Head of Internal Whistleblowing Systems* may share with the Whistleblower only information strictly necessary to carrying out his or her activity. The identity of the Whistleblower, where known, can only be disclosed with his or her express consent to persons other than those responsible for receiving or following up reports, expressly authorised to process the data. Without this consent, no information, fact or evidence that might allow the whistleblower to be identified can be disclosed, unless it has first been anonymised.

During the investigation, the *Head of Internal Whistleblowing Systems* examines the circumstances through an analysis of the available documents and data and, where deemed useful/appropriate, by interviewing the Whistleblower and all other persons deemed useful to resolving the case.

Investigations must be conducted in a professional manner, in accordance with all applicable rules on the rights of defence of the persons concerned.

If a report has been made by telephone or another voice-messaging system, the oral report must be documented by:

- with consent, a recording of the conversation on a device appropriate to storage and play-back; or
- a complete, accurate transcription of the conversation with the designated person; this latter option must enable the Whistleblower to verify, modify and approve the transcription of the call with a signature.

If the whistleblower requests to meet the *Head of Internal Whistleblowing Systems*, the meeting must be documented:

- with consent, by a recording of the conversation on a device appropriate to storage and play-back; or
- an accurate minute of the meeting that enable the Whistleblower to verify, modify and approve it with a signature.

During the investigation, all documentation must be stored in a durable form that enables easy access to information, in accordance with data protection requirements and for the time required to complete the investigation.

In addition, the *Head of Internal Whistleblowing Systems*:

- maintains discussions with the Whistleblower, from whom additional information may be requested, where necessary;
- provides the Whistleblower with formal, well-founded responses, which must be the result of a thorough assessment of the facts;
- provides a feedback to the report within three months of the date of notice of receipt or, in the absence of such notice, within three months of the end of the period of seven days from the submission of the report.

Where a report is considered an actual breach of the applicable rules, the *Head of Internal Whistleblowing Systems*, with the involvement of the Head of the Internal Audit Department and any other structures that have supported the performance of the investigation, produces a report on the breach.

Breaches of high severity, concerning particularly significant unlawful conduct, in view of the underlying conduct and/or the professional concerned, must be immediately reported to the Chief Executive Officer, Board of Directors and Board of Statutory Auditors, which will examine them at the next available session.

By way of example and without limitation, unlawful acts and actions include:

- breaches that lead to the presumption of losses or lost revenues;
- breaches that result in liability for administrative and/or criminal penalties from the competent judicial and supervisory authorities;
- breach of the provisions of Legislative Decree No. 231/2007, as further amended, with particular regard to the obligation to report suspicious transactions, customer due diligence obligations and the obligation to record transactions and ensure record-keeping.

3.7. DEFINITION OF REMEDIAL MEASURES

The *Head of Internal Whistleblowing Systems*:

- identifies, in concert with all other competent functions, and in particular with the Head of the Internal Audit Department, any remedial measures to be implemented (interventions on processes, procedures or control safeguards) and their timeframes;
- assesses whether disciplinary penalties should be proposed, in accordance with the law and the national labour contract;
- sends the findings obtained to those responsible for decision-making for the assessment of any disciplinary measures to be taken;
- in case of violations of particular severity, sends the Report to the Chief Executive Officer, Board of Directors and Board of Statutory Auditors, after notifying the Internal Audit Department, whereas in case of violations relevant for the purposes of Legislative Decree No. 231/2001, sends it to the Supervisory Board;
- gives notice of the outcome of the Report, in concise form, to the whistleblower along with — where disciplinary penalties are not envisaged — the person subject to the report. Where disciplinary penalties are envisaged, the decision-makers are tasked with informing the person subject to the report.

Where the Whistleblower is jointly liable for breaches, privileged treatment must be applied to the Whistleblower in respect of the other jointly liable parties, in accordance with the applicable legislation. The parties responsible for decision-making measures must be given adequate information on this account.

3.8. DECISION-MAKING MEASURES

The decision regarding measures to be taken against personnel involved in breaches falls to:

- for employees of the Parent Company and/or other Banking Group companies, the Human Resources Department, after having heard the body with managing functions (Chief Executive Officer and General Manager, Managing Director), as such Department is in charge of implementing disciplinary proceedings against employees;
- for Financial Advisors, the Disciplinary Committee provided for in the specific internal circular;
- for members of Company Bodies, the Board of Directors and/or the Board of Statutory Auditors, as the case may be, which, each within its purview, may take the most appropriate and adequate initiatives, in keeping with the severity of the breach and in accordance with the powers envisaged in the law and/or the Articles of Association;
- for third parties (suppliers, consultants, etc.), the body with managing functions (Chief Executive Officer and General Manager, Managing Director), which decides on a case-by-

case basis the measures to be implemented (e.g., termination of the supply/consultancy agreement, etc.).

3.9. MONITORING

The Head of the Compliance and Anti-Financial Crime Department and the Head of the Internal Audit Department monitor that any corrective measures identified are effectively implemented on the agreed timescales. Where the corrective measures relate to violations concerning anti-money laundering and prevention of financing of terrorism, monitoring is conducted with the support of the Head of Anti-Financial Crime function, who submits a report on the subject periodically to the Head of the Compliance and Anti-Financial Crime Department.

3.10. PROTECTION AND ANTI-RETALIATION MEASURES

All reports are processed and classified with the highest level of confidentiality, and the confidentiality and protection of the personal data of the whistleblower and the person concerned, if any, are always ensured[1].

The Bank ensures the confidentiality of the Whistleblower's identity, except for the cases where:

- the Whistleblower consents to disclose it;
- disclosure is required by law (e.g., the information requested is necessary for investigations or proceedings initiated by a judicial authority following a report);
- knowledge of it is indispensable to the defence of the person concerned.

Whistleblowers acting in good faith are guaranteed and protected against all forms of retaliation, discrimination or penalisation, regardless of the parties involved.

The Whistleblower may not be subject to conduct that is retaliatory, discriminatory or otherwise unfair for having made a report. All forms of retaliation or harassment are prohibited and may therefore give rise to disciplinary measures.

Protection measures also apply to facilitators and other parties closely related (by family and/or working relationships) to the Whistleblower pursuant to Legislative Decree No. 24/23.

A Whistleblower who reports externally to the competent authorities shall qualify for protection against retaliation, when the Whistleblower:

- first reported internally, but no follow-up was undertaken;
- has reasonable grounds to believe that, in case of internal reporting, there is a low prospect of the breach being effectively addressed or there is a risk of retaliation,
- or has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest.

A Whistleblower who makes a public disclosure shall also qualify for protection against retaliation, when the Whistleblower:

- first reported internally and externally, or directly externally, but no feedback was given within the terms established about the action envisaged or taken as follow-up;
- has reasonable grounds to believe that the external reporting may entail a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular

[1] Confidentiality obligations do not apply when the information requested is necessary for investigations or proceedings initiated by a judicial authority following a report.

circumstances of the case, such as those where evidence may be concealed or destroyed or where the recipient of the report may be in collusion with the perpetrator of the breach or involved in the breach;

- or has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest.

This is without prejudice to the facts that reports must be supported by specific facts and founded on precise, concordant factual elements.

All forms of abuse of this Policy, such as reports made solely to harm the person concerned or other parties, and all other cases of improper use or intentional abuse of the whistleblowing system, may give rise to disciplinary liability.

All documents regarding the reports are confidential. Such documentation must be securely stored in accordance with applicable rules in effect at the Bank regarding the classification and processing of information and in compliance with local laws and regulations[2]. This documentation must be stored at the Department of the Head of Whistleblowing and at the Function that has conducted the verification, and must be, in any event, made available solely to authorised employees.

3.11. DISCLOSURE AND REPORTING OBLIGATIONS

The *Head of Internal Whistleblowing Systems* ensures the availability of clear information regarding internal whistleblowing systems, procedures and requirements for reporting internally, as well as on the reporting channel, procedures and requirements for submitting reports to the Italian National Anti-Corruption Authority (ANAC)[3].

To this end, this Policy and the above-mentioned information are published in the website bancagenerali.com and on the company Intranet.

Each year, the *Head of Internal Whistleblowing Systems* drafts a report on the proper functioning of internal whistleblowing systems containing aggregate information regarding the results of the activity performed following the reports received.

The report is then made available to the Bank's Personnel in a dedicated section of the company Intranet[4].

[2] Personal data that manifestly is not useful to the processing of a specific report is not collected or, if accidentally collected, is immediately deleted. Reports and the related documentation are stored for the time necessary to process the report and, in any case, for no longer than five years from the date of the final outcome of the reporting procedure.

[3] Pursuant to Article 6 of Legislative Decree No. 24/23.

[4] Circular No. 285 of 17 December 2013 (Title IV, Chapter 3, Section VIII): "In accordance with the provisions set forth by data protection regulations, each year the head of internal whistleblowing systems drafts a report on the proper functioning of internal whistleblowing systems containing aggregate information regarding the results of the activity performed following the reports received. This report is approved by the corporate bodies and made available to the bank's personnel."