Generali Real Estate S.p.A.

WHISTLEBLOWING POLICY

Generalirealestate.com

Approved by	Board of Directors of Generali Real Estate S.p.A.
Effective date	*2023-07-15*

Annexes

ANNEX I – CATEGORIES OF ISSUE TYPES
ANNEX II – PROHIBITED RETALIATORY PRACTICES

Contents

1 Executive Summary

Objective of the document	*This Policy illustrates the measures adopted by GRE for the management of Whistleblowing, providing a whole guidance for everyone who witnessed or experienced a breach of the Organization and Management Model, Code of Conduct or of other internal or external regulations on how to report it by:* • *defining the reporting of concerns management process;* • *removing factors that may hinder or discourage concerns reporting, providing the reporter (whistleblower) with clear indications about contents, recipients and methods of transmission of the concern;* • *providing protection to the whistleblower;* • *defining roles and responsibilities.*
Scope of application	*The document applies to Generali Real Estate S.p.A.*

In consideration of the activities governed by this Internal Regulation and its potential impacts, it is also relevant for the purposes of Legislative Decree 231/2001. Therefore, the breach of its provisions will constitute a breach of the Organization and Management Model and penalties may be imposed in accordance with the provisions of the Model itself. Anyone who becomes aware of a potential breach of the Organization and Management Model is required to promptly inform the Supervisory Body established pursuant to Legislative Decree 231/2001.

2 Glossary and Definitions

Acronym/ Term	Explanation/Definition
ANAC	Italian Anti-corruption Authority
Board of Directors (BoD)	Board of Directors of GRE
Breach (or violation)	An actual or potential practice or conduct which is inappropriate or inconsistent with the law, the Code of Conduct or other internal regulation, which occurred or is very likely to occur Please refer to Annex I for the specific violations considered by local regulations.
Compliance Officer	Head of the A&WM BU Compliance Function
Concern	Knowledge or reasonable suspicion about a practice or conduct considered, in good faith and without gross negligence, as inappropriate or inconsistent with the law, the Code of Conduct or other internal regulation
Employees	Persons who, for a certain period of time, perform services for and under the direction of the Generali Group, in return for which they receive remuneration. Thus, those include workers in non-standard employment relationships, including part-time workers and fixed term contract workers, as well as persons with a contract of employment or employment relationship with a temporary agency and precarious types of relationships.
Ethics Point	The case management system
Facilitator	A natural person who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential.
Generali Group (or Group)	The Generali Group whose ultimate parent Company is Assicurazioni Generali S.p.A.
Generali Group Whistleblowing Tool (or Group Whistleblowing Tool)	The official internal reporting tool managed by the Group Ethics & Investigations structure to allow any person to report Concern to the Group Legal Entities in compliance with the EU Whistleblower Protection Directive. This tool has a component which provides access to the Reporters (i.e., Group Whistleblowing Helpline) and a component which provides access and case management exclusively to the authorized persons such as the Compliance Officers (i.e., Group Whistleblowing Case Management System). This tool is hosted by a third-party provider on servers located within the European Union.
GRE	Generali Real Estate S.p.A.
Group Compliance Helpline (or Helpline)	Internal violation reporting system
Information on violations	Information, including reasonable suspicion, concerning violations committed or which, on the basis of concrete elements, could be committed in the organization with which the Reporter or the person making the complaint to the judicial or accounting authority has a legal relationship, as well as elements concerning conduct aimed at concealing such breaches
Surveillance Body	Internal Control Body, responsible for supervising the functioning of and compliance with the Organization and Management Model, as well as for updating it
Personal Data	Any information directly or indirectly relating to an identified or identifiable natural person

Person Concerned (or Reported)	The person described by the Reporter as the perpetrator of the violation of one or more principles of the Code of Conduct, internal and external regulations or the person otherwise involved in the reported or publicly disclosed violation
Public Disclosure	A situation in which a person makes information available in the public domain, for instance, directly to the public through online platforms or social media, or to the media or otherwise through means of dissemination capable of reaching a large number of people, elected officials, civil society organizations, trade unions, or professional and business organizations.
Report	A communication concerning the reasonable and legitimate suspicion or awareness of wrongdoing, malpractice or any illegal or unethical conduct that can harm the business and the reputation of GRE or the Group as a whole and that, for the purposes of L.D. 24/2023 only, consist in the violations considered by L.D. No. 24/2023 and listed above.
Reporter (Whistleblower)	Reporters (or Whistleblower or Reporting Person) is a person who speaks up on good faith and without gross negligence when he/she encounters, in the context of the work, wrongdoing, malpractice or any illegal or unethical conduct that could harm the business and the reputation of GRE or the Group as a whole. As far as GRE is concerned, the following subjects are considered as Reporters for the purposes of Legislative Decree no. 24/2023: a) subordinate workers of entities, including workers whose employment relationship is governed by Legislative Decree no. 81, or by article 54-bis of the decree-law of 24 April 2017, n. 50, converted, with amendments, by the law of 21 June 2017, no. 96; b) self-employed workers, including those indicated in chapter I of the law of 22 May 2017, n. 81, as well as the holders of a collaboration relationship referred to in article 409 of the code of civil procedure and in article 2 of legislative decree n. 81 of 2015, who carry out their work for subjects in the public sector or in the private sector; c) workers or collaborators who carry out their work for subjects in the public sector or in the private sector who supply goods or services or who carry out works on behalf of third parties; d) freelancers and consultants who work for entities in the public or private sector; e) volunteers and trainees, paid and unpaid, who work for entities in the public or private sector; f) shareholders and persons with administrative, management, control, supervisory or representative functions, even if these functions are exercised purely de facto, with subjects in the public sector or in the private sector.
Retaliation	Any conduct, act or omission, even if only attempted or threatened, committed by reason of the Report, the complaint to the judicial or accounting authorities or the public disclosure and which causes or is likely to cause the reporting person or the person making the complaint, directly or indirectly, unjust damage.
Whistleblowing	Reporting system for violations
Work-related context	Any current or past work activities through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer Retaliation in the event of internal or external reporting, public disclosure or reporting to the judicial or accounting authorities.

3 Roles and Responsibilities

Role	Responsibilities	Section / Paragraph
CEO	▪ ensures that employees are protected against any form of retaliation because of reporting concerns in good faith.	5.5
Local Senior Management	▪ ensures that adequate resources - human capital, expertise, information technology and other - are dedicated to manage the reporting of Concerns and the investigations; ▪ ensures that the channels for reporting violations of the Code of Conduct and other internal regulations are available to all Employees and third parties; ▪ ensures that all the relevant personnel receive adequate information and training on the reporting of Concerns.	5.1
Group Compliance Officer Function	▪ manages the Group Whistleblowing Tool in collaboration with the BU/ Local Compliance Officer; ▪ manages the Concerns within his/ her perimeter of responsibility and coordinates and supervises the management of the Concerns among the Group; ▪ submits the proposal for disciplinary sanctions (or other relevant remedial measures) to the competent level of authority (e.g., GCEO, Chairman of the AG BoD) for final decisions; ▪ monitors that any form of Retaliation occurs as a result of a Concern highlighted by an Employee.	5.8
Compliance Officer	▪ manages the Concerns within his/her perimeter of responsibility; ▪ provides advice to the Senior Management in managing the consequences of the reporting and related investigation supporting also the decisional process to identify the most appropriate remedial measures; ▪ submits the proposal for disciplinary sanctions (or other relevant remedial measures) to the competent level of authority (e.g., CEO, AMSB) for final decisions; ▪ monitors that any form of Retaliation occurs as a result of a Concern highlighted by an Employee; ▪ must timely store the managed reports received and all related information into the Group Whistleblowing Case Management System. ▪ monitors that no retaliation occurs as result of a concern highlighted by an employee	5
Internal Audit Function	▪ supports the Compliance Function, upon request, in managing investigations; ▪ supports the Compliance Function, upon request, in verifying that the approved remedial measures following a concern are effectively implemented.	6
Human Resources Function	▪ identifies the appropriate remedial measures to be applied case by case and in preventing retaliatory actions; ▪ submits the proposal for disciplinary sanctions (or other relevant remedial measures) to the BoD for final decisions; ▪ submits grounded Concerns and/ or identified Breaches to the Compliance Officer timely.	5; 6

Surveillance Body	▪ supervises and, where requested by the person responsible for the report, supports the activities of analysis and verification of the content of the report. ▪ evaluates the outcome of the investigations carried out by the reporting manager. ▪ involves, if necessary, of the relevant HR function.	5.7; 5.8; 6
Employee	▪ performs his/ her duties with professional due diligence, care and good faith in compliance with the provisions of the Group Code of Conduct; ▪ supports with care the internal and external investigations providing true and accurate information when requested by the Compliance Officer(s), by any person appointed to conduct the investigation or by any competent authority(ies); ▪ submits a Concern when he/she becomes aware of any Breach.	All

4 Introduction

4.1 REGULATORY FRAMEWORK

This Policy has been prepared taking into the current legislative framework as well as the Code of Conduct.

In this regard, Legislative Decree no. 24 of 10 March 2023 "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws" (**Decree 24**) has introduced a uniform discipline on the reporting of law violations without prejudice of the reporting systems introduced by any other additional and/or sectoral regulations.

In accordance with the abovementioned internal and external regulatory sources, this Policy sets-out:

- the rules for the internal management of reports concerning acts or facts which may constitute a violation of internal regulations (Organisation and Management Model, related regulations and Code of Conduct) and of the law applicable to GRE (so-called internal whistleblowing), including with reference to Decree 24;
- two types of reporting channels, internal and external, as well as, pursuant to Decree 24, the possibility to make "public disclosure" for the violations envisaged by the same Decree; and
- a protection measures system for the Reporter and other individuals or entities related to him/her on his/her internal or external Reports, complaints to the judicial or accounting authorities and public disclosures.

This Policy is exposed and made easily visible in the workplace, published on a specific section of the Company's website as well as on the Company intranet and made accessible to persons who have a legal relationship pursuant to Article 3(3) and (4) Decree 24.

The above requirements are part of a broader regulatory framework related to the General Data Protection Regulation (GDPR) which provides for the protection of all personal data processed at each stage of the reporting process.

4.2 APPROVAL AND REVIEW

This Policy is approved by the Board of Directors upon proposal of the CEO.

This document is promptly reviewed, in any case at least every three years, to include developments in legislation, market and/or best practices, GRE strategy and organization.

The A&WM BU Compliance Officer is delegated by the Board of Directors to approve Minor Changes.

4.3 EFFECTIVE DATE AND IMPLEMENTATION

The Effective Date as well as the Implementation Deadline of this Policy is 15 July 2023.

4.4 IMPLEMENTATION, MONITORING AND INFORMATION FLOWS

Any relevant organizational unit shall promptly inform BU Internal Audit, BU Risk Management and BU Compliance Officer of any facts and/or circumstances connected with this Policy, which may be relevant for the performance of their duties.

5 Reporting Concerns

5.1 REPORTING PRINCIPLES

The Group fosters an ethical culture which values and actively encourages the contribution from the Employees to reinforce and protect the integrity of our work environment. The internal reporting process (i.e., whistleblowing) is an essential part of the internal control system aimed to reinforce a positive communication and corporate social responsibility as a Reporter can significantly contribute to self-correctness and excellence within the Generali Group.

The whistleblowing process provides safe and confidential channels for reporting any Concerns and it is designed to facilitate the detection and management of violations of our Code of Conduct (e.g., harassment, discrimination, mobbing) which could affect the single Employee and the work environment. At the same time, the whistleblowing process is critical to detect, discourage and prevent serious misconduct and breaches of law, and the related damages including direct losses (e.g., administrative sanctions, costs of defense, additional controls to be implemented, disruption of the business activities) and reputational impacts for the Company and the entire Group.

In this context, the Senior Management must ensure that adequate resources – human capital, expertise, information technology and other – are dedicated to implement this Policy, support the investigations, and ensure that all personnel receive adequate information and training on the reporting of Concerns and the provisions set by this Policy.

The CEO must cooperate to ensure that the Compliance Officer has access to all internal information relevant to the investigation which are available in the Company (e.g., HR report) in accordance with local applicable regulations.

At the same time, Employees must perform their duties with professional due diligence, care, and good faith in compliance with the provisions of the Group Code of Conduct and the Company's Code of Conduct, making themselves aware of Code of Conduct provisions and of the internal regulations applicable to their tasks.

In accordance with the duties of diligence and loyalty, Employees must report a Concern when they become aware of any Breach and support with due care the internal and external investigations by timely providing true and accurate information when requested by the Compliance Officer, by any person appointed by the Compliance Officer to conduct the investigation or by any competent authority(ies).

A person will be subject to disciplinary measures, including termination of employment and may also result in civil and/or criminal sanctions, in accordance with local law and internal regulations, if he/she:

- violates internal and external requirements;
- commits retaliation against the whistleblower or other persons related to him and protected by Decree 24;
- obstructs or attempted to obstruct reporting;
- violated the obligation of confidentiality;
- the criminal liability of the reporting person for the crimes of defamation or slander or in any case for the same crimes committed with the report to the judicial or accounting authority is ascertained, even with a first instance sentence, or his/her civil liability, for the same reason, in cases of willful misconduct or gross negligence;
- the reporting channels or procedures for making and managing reports have not been adopted or if these procedures do not comply with articles 4 and 5 of Decree 24;
- the verification and analysis of the Reports received has not been carried out.

5.2 WHO MAY REPORT

Anyone (Employees, vendors, consultants, other stakeholders) who has experienced or witnessed a Concern may report it as better specified in the following paragraphs.

All Employees shall actively collaborate in identifying any situation that could expose GRE and the entire Group to reputational risks and/ or economic losses.

Reported Concerns are classified according to the Issue Types and examples listed in Annex II. This classification is also aimed at helping the Reporter in realizing if something wrong is going on and should be reported.

Reports must be circumstantiated, reasonable and meaningful, and cannot be based on a prejudice or a bias. They should contain the necessary details to allow an investigation. Reports without sufficient information, such as the description of the circumstances of the alleged violation, cannot trigger an investigation and will need to be followed up to collect the sufficient information to ground an investigation.

The Reporters are expected to collect and organize the relevant information in order to facilitate the internal investigation by providing a clear and sufficient picture to support the understanding of the case and allow an impartial and fair investigation by the competent function.

The Reporters should disclose any personal/ private interest connected to the allegation that may influence their personal judgment/ objectivity.

5.3 WHAT SHOULD/SHOULD NOT BE REPORTED

GRE encourages to report any practice or conduct that it is considered, in good faith and without gross negligence, as inappropriate or inconsistent with the law, the Organization and Management Model, other internal regulations and the Code of Conduct.

All the reporting channels (indicated below) are open for reporting to any kind of Concern, also including behavior of suppliers, outsourcers and anyone acting on behalf of/in connection with the Group.

Reports should be circumstantiated: they should contain the necessary details to ground an investigation although it is not necessary to have evidence of the facts reported. Reports without sufficient information such as the description of the circumstances of the alleged violation, cannot be examined.

The following are excluded from the scope of this Policy and the Group Compliance Helpline:

- requests for commercial information or complaints from clients and/or investors;
- reports from Employees dissatisfied with their performance evaluation/career path unless connected with diversity and inclusion, harassment or retaliation issues;
- reports related to aspects of personal life which are not connected to the working activities.

Furthermore, the provisions of Decree 24 do not apply to:

- disputes, claims or demands related to an interest of a personal nature of the reporting person or the person making a report to the judicial or accounting authority that pertain exclusively to their individual labor or public employment relationships, or inherent in their labor or public employment relationships with hierarchically subordinate figures;
- reports of violations where they are already mandatorily regulated by the European Union or national acts indicated or by national acts that constitute implementation of the European Union acts indicated in Part II of the Annex to Directive (EU) 2019/1937, although not indicated in Part II of the Annex to Decree 24;
- reports of national security breaches, as well as procurement related to defense or national security aspects, unless such aspects are covered by relevant secondary legislation of the European Union.

Any such Report will not be considered relevant under this Policy and, therefore, will not be examined.

5.4 WHAT TO DO

When a person assists or becomes aware of any Breach or has a concern that a Breach can occur, he/ she should write down what happened (e.g., dates, times, places, situations, witnesses) and keep licit evidence of the inappropriate conduct (e.g., documents, written conversations).

In case of harassment (which is determined by how a person individually perceives other people actions regardless of the original intentions), when a person believes to have been subjected to an inappropriate conduct before the case is reported, he/ she should make clear to the involved person that such conduct is perceived as offensive and should stop. Indeed, if the colleague is in good faith, she/ he should recognize the colleague's perception and apologize for that. On the other hand, if the harassment persists or when there is a fear of Retaliation, a Concern should be reported accordingly with this Policy.

All Employees are recommended to employ human touch (i.e., partner with others, showing empathy and team spirit) to overcome disputes. Employees shall always use respectful attitudes with all people they work with.

5.5 RIGHTS AND OBLIGATIONS OF THE REPORTER

Employees and others are encouraged to feel safe to engage in frank, honest communication raising questions or Concerns at any time without fear of retaliation.

Any Report must be made in good faith and without gross negligence.

The Reporter should disclose any personal/private interest connected to the allegation that may influence his/her personal judgment/objectivity.

The Reporter can decide to report anonymously. In this case, the Helpline provides the Reporter with an ID code to allow the exchange of information with the Compliance Officer. Although anonymous reports are accepted, GRE encourages to disclose the identity while submitting a Report, as this usually allows a more effective investigation.

The content of the Reports, the Reporter's personal data (such as the name, surname, email address) and that of the other individuals involved, will be processed confidentially with utmost discretion by the Compliance Officer and any other person involved in the process, and in compliance with the GRE Privacy Policy and any applicable personal data protection regulation.

The Compliance Officer ensures to keep the identity of the Reporter:

- confidential, when the Reporter is known (i.e., the Company will not reveal the Reporter's identity without explicit consent);
- anonymous, when the identity of the Reporter is not known or otherwise identifiable.

The legal provision under which the Person Concerned has the right to obtain, among other things, an indication of the origin of personal data (art. 15 of General Data Protection Regulation UE no. 2016/679) does not apply to the identity of the Reporter, which may only be disclosed with his/her consent. More generally, the rights of the interested party referred to in articles from 15 to 22 of Regulation (EU) 2016/679 can be exercised if such exercise cannot result in an effective and concrete prejudice to the confidentiality of the Reporter's identity.

Furthermore, within the context of disciplinary proceeding following a Report:

A. the identity of the reporting person may not be disclosed, where the allegation of the disciplinary charge is based on investigations and additional to the report, even if consequent to the Report;
B. where the allegation is based, in whole or in part, on the Report and knowledge of the identity of the Reporter is indispensable for the defense of the accused, the Report will be usable for the purposes of the disciplinary procedure only with the express consent of the Reporter.

The Reporter shall be notified in written communication of the reasons for the disclosure of the confidential data in the case referred to letter B. above as well as in the internal reporting procedures when the disclosure of the Reporter's identity and of information from which his/her identity can be directly or indirectly inferred, is also indispensable for the defense of the person involved.

Any person who may hinder or attempt to hinder reporting or breach the duty of maintaining the confidentiality of the Reporter's personal data and of the other persons involved will be passive of disciplinary measures.

Violations, as well as reporting in bad faith, are subject to disciplinary measures, including termination of employment, and may also result in civil and/or criminal sanctions, in accordance with local law and internal regulations.

GRE ensures that Employees are protected against any form of retaliation because of reporting Concerns in good faith and without gross negligence.

Retaliation is misconduct where someone acts in an unfair or negative way against someone who:

- reports in good faith and without gross negligence;
- supports another person's Concern;

- collaborates in the investigation of Concerns.

Retaliation can include harassment, intimidation, discrimination for engaging in protected activities such as reporting violations or participating in an investigation pertaining to alleged violations of the law, Organization and Management Model, other internal regulation or the Code of Conduct. By way of example, below there is a no exhaustive list:

- employment actions, such as termination, denial of promotion, demotion, job duties changes or pay cut;
- other actions affecting employment or having however a negative impact such as threats, unjustified negative evaluations, unjustified negative references, increased surveillance or failure to ensure the employees' safety in the workplace;
- harassing and mobbing, including ignoring and avoiding the Employee in an obvious manner, failing to provide the Employee with important information needed to perform his/her job or blaming the employee for causing problems because he/she filed a Concern or remaking that the employees should transfer or quit the job;
- physical harm.

It can manifest itself in a verbal, physical or written form.

The Reporter is protected against retaliation even if the Concerns raised are not confirmed following an investigation.

However, Employees are not exempted from the consequences of their own misconduct such as knowingly making false allegation, provide false or misleading information in the course of an investigation or act in bad faith. Any abuse of the process by the Reporter to obtain a personal advantage or simply to slander or libel the Person Concerned are not tolerated.

Feedback is provided to the Reporter by Compliance Officer within three months from the communication of receipt of the Report. The Reporter can follow-up, sending and receiving communications, on the progress of the case.

5.6 TO WHOM REPORT

The person who in good faith and without gross negligence believes to have suffered or witnessed a Breach should report the Concern to the Compliance Officer, at Local or Group Level.

The Compliance Officer, as responsible person of an independent control function, ensures the management of Concerns and of related investigations in a professional manner, in accordance with the provisions of this Policy and also receives a dedicated training to adequately perform the activities and tasks described in this Policy.

Before reporting to the Compliance Officer, it is up to the Reporter to evaluate whether he/she deems useful or appropriate to preliminarily share the relevant Concern with his/ her Direct Manager or with the HR Function in order to allow such persons to act as Facilitators. In case the Reporter effectively evaluates such opportunity, the Direct manager and the HR Function involved must record the information related to the Concern in writing on a durable medium, documenting the related evaluations to demonstrate the active support provided to the Reporter.

It is critical that any relevant information is swiftly submitted to the persons closest to the source of the problem: their investigation and power to remedy are, in most of the cases, more effective and they can investigate and propose to adopt the proper measures timely. This principle is established to foster a culture of good communication and corporate social responsibility.

If the Report is submitted through the Generali Group Whistleblowing Tool, an automatic procedure assigns the case to the Compliance Officer closest to the events. This procedure escalates to the higher-level Compliance Officer in case of conflicts with the Local Compliance Officer or the Local Senior Management in order to ensure impartial investigation.

If the Reporter is anyway not comfortable to share his/ her concern at Local level, he/ she is encouraged to report directly to the Group Compliance Officer by writing to the concerns.co@generali.com or contacting the Group Ethics & Investigations structure.

Local Senior Management must provide clear and easily accessible information regarding the provisions set by this Policy and the procedures for reporting externally to competent authorities in compliance with applicable regulations.

The above is in addition to the Compliance Helpline.

The channels managed by the Compliance Officer must be always preferred and used to manage the reporting processes in order to ensure the effectiveness and the consistency of the investigations if compliant with the local requirements.

5.7 THE COMPLIANCE OFFICER ROLE

The Compliance Officer is the person in charge of receiving, examining and assessing reports. The Compliance Officer does not take part in the adoption of any disciplinary measures and reports directly and without delay to the Board of Directors, Boards of Auditors and to Surveillance Body the information reported, where relevant. When requested by the Reporter, the information being reported is brought to the attention of the corporate bodies, guaranteeing the Reporter's anonymity.

The Compliance Officer is also nominated as responsible for the internal reporting systems and in this role has to ensure that the procedure is carried out correctly.

GRE Compliance Officer and has the duty to

- ensure the proper conduct of the process of reporting violations;
- report directly and without delay to Board of Directors the information reported, where relevant, and;
- draw up an annual report to be included in the annual compliance report on the correct functioning of the internal reporting systems, in compliance with the provisions of the regulations on the protection of personal data, containing aggregate information on the results of the activities carried out following the Reports received; the report shall be approved by the corporate bodies and made available to the Employee.

The Compliance Officer – in conjunction with the HR Department - has the duty to monitor and control that, during and after the investigation, any form of retaliation does not occur as GRE strictly prohibits any form of retaliatory action against Employees who raise issues or ask questions, make Reports, participate in an investigation, refuse to participate in suspected improper or wrongful activity.

If the Compliance Officer – in conjunction with HR Department - verifies the occurrence of a retaliation against a Reporter or anyone who has supported or collaborated with the Reporter or in the process of the investigation, Human Resources:

- identifies any remedial measures (of organisational, procedural nature, etc.) to be implemented;
- evaluates whether disciplinary sanctions are appropriate, considering local law and internal regulations;
- will take immediate initiative for submitting the proposal for disciplinary sanctions (or other relevant remedial measures) to the Board of Directors for final decisions (form penalties up to employment termination).

5.8 HOW TO REPORT (REPORTING CHANNELS)

INTERNAL REPORTING CHANNELS

Reports can be made personally or anonymously, in writing or orally.

There are several alternative channels to contact the Compliance Officer:

- directly in person,
- by e-mail: chiara.petronzio@generali.com;
- by post: Assets & Wealth Management BU Compliance Officer (Chiara Petronzio) – Piazza Tre Torri 1, 20145, Italy.
- by the Generali Group Compliance Helpline at https://generali.whispli.com/speakup;
- the Group Whistleblowing Helpline available at the Generali Group website (https://www.generali.com/ourresponsibilities/responsible-business/code-of-conduct) by phone or web;
- post: Group Compliance – Group Ethics & Investigations – V. Machiavelli 3, 34132 Trieste, Italy.

The URL address of the Generali Group Compliance Helpline can be found on the Group Corporate Web site (www.generali.com), on the Group Portal “WE, Generali” and on the local intranet sites.

To this end, the Company may, where appropriate, enter into intra-group agreements to define the respective responsibilities for compliance with data protection obligations, pursuant to Article 26 of Regulation (EU) 2016/679.

The Helpline is a specific, autonomous and independent tool that differ from ordinary reporting lines and is hosted by an independent third-party provider that ensure appropriate levels of confidentiality of information. The Helpline is managed by the Group Compliance Officer Function.

The Group Whistleblowing Helpline accepts Reports in all the languages of the countries where the Generali Group operates and all the phone numbers to be contacted are made available. The Group Whistleblowing Helpline is hosted by an independent third-party provider and managed by the Local and Group Compliance Function. Cases reported via the Group Whistleblowing Helpline are automatically assigned to the appropriate Compliance Officer. This channel shall not be used in case of emergency situations or events presenting an immediate threat to life or property. In those cases, please immediately contact relevant local authorities.

If the Concern regards the Compliance Officer, it is possible to contact the Group Compliance Function:

- by the Generali Group Compliance Helpline at https://generali.whispli.com/speakup, by phone or web;
- by e-mail: concerns.co@generali.com;
- by post: Group Compliance – Business Integrity – V. Machiavelli 3, 34132 Trieste, Italy.

Moreover, to facilitate the specific reporting of violations of the Organization and Management Model, including potential ones, the Company makes available the following communication channels:

- a dedicated e-mail box: odv231_GRE@generali.com;
- an address to which written reports may be forwarded: Via Machiavelli, 4, 34132 Trieste (TS), for the attention of the Chairman of the Surveillance Body.

Where a case is reported via a local channel, the local Senior Management ensure that reports are referred to the local Compliance Officer within 7 days of receipt and simultaneously give notice of the transmission to the Reporter. The Compliance Officer who receives a Concern via any channel other than the Group Whistleblowing Case Management System must upload its key elements and related documentation, including the original Report (sanitized if needed), in the Group Whistleblowing Case Management System timely (i.e., maximum within 3 working days), as a register of reports, in compliance with local applicable regulations.

In the case of a Report received directly by the Surveillance Body (through the appropriate reference channel indicated above), the Surveillance Body must promptly inform the Compliance Officer, so that it can carry out the checks on the procedural aspects in accordance with what is described in the following paragraphs.

In the event that the Surveillance Body is the direct recipient of reports for which it believes it is not competent, it shall promptly forward the contents to the Compliance Officer in accordance with this Policy.

The channels indicated above are the only ones foreseen for sending the reports covered by this Policy. The use of other channels does not guarantee that they will be received and dealt with.

For more information, the Reporters are invited to refer to the Compliance Officer or the relevant internal regulations.

EXTERNAL REPORTING CHANNELS

External Report of violations pursuant to Decree 24

The Reporter may make an external Report if, at the time of its submission, one of the following conditions are met:

a) there is no mandatory activation of the internal reporting channel within his or her work context or this channel, even if mandatory, is not active or, even if activated, does not comply with the provisions of Article 4 of L.D. No. 24/2023;
b) the Reporter has already made an internal Report and it has not been followed up;
c) the Reporter has reasonable grounds to believe that if he or she used an internal reporting channel, the Report would not be effectively followed up or that the same Report may result in the risk of retaliation;
d) the Reporter has reasonable grounds to believe that the violation may pose an imminent or obvious danger to the public interest.

To this end:

- the Italian National Anti-Corruption Authority ("**ANAC**") activates an external reporting channel that ensures, including through the use of encryption tools, the confidentiality of the identity of the Reporter, the person involved, and the person mentioned in the Report, as well as the content of the Report and related documentation;

- external reports shall be made in written form through the IT platform or orally through telephone lines or voice messaging systems or, at the request of the Reporter, through a face-to-face meeting set within a reasonable time period;
- an external report submitted to a person other than ANAC shall be transmitted to ANAC, within seven days from the date of its receipt, giving simultaneous notice of the transmission to the reporting person.

Please refer to ANAC website for further information.

Public disclosures according to Decree 24

The reporting person making a public disclosure shall benefit from the protection provided for in L.D. No. 24/2023 if, at the time of the public disclosure, one of the following conditions is met:

a) the Reporter has previously made an internal and external Report or has made an external Report directly, under the conditions and in the manner laid down in Articles 4 and 7 of L.D. No. 24/2023 (see previous paragraphs), and no reply has been received within the prescribed time limits on the measures envisaged or taken to follow up the reports;
b) the Reporter has reasonable grounds to believe that the breach may constitute an imminent danger or clear danger to the public interest;
c) the Reporter has justified reason to believe that the external Report may involve the risk of retaliation or may not be effectively followed up because of the specific circumstances of the case, such as those where evidence may be concealed or destroyed or where there is a well-founded fear that the recipient of the report may collude with the infringer or be involved in the breach itself.

6 Management of the Reports

A Report is considered relevant if it relates to one or more of the following:

- facts that may include Breaches, crimes, offences, irregularities;
- actions that may cause significant damage to the Company's assets or reputation;
- actions likely to cause damage to the health or safety of employees or the environment;
- actions carried out in violation of the Code of Conduct or other provisions or internal procedures that may be subject to disciplinary action.

Whoever receives a Concern must treat it with the utmost confidentiality and share information only on a need-to-know basis.

Every Report will be taken into due account.

When submitting a concern, the Reporter should indicate at least the following elements to support the process for the assignment of the case:

- Country(ies) in which the Reporter is located;
- Country(ies) in which the events or the Breach occurred;
- Group Legal Entity(ies) in which the violation occurred;
- Whether the case involves the Senior Management and/ or the Compliance Function of the Company in which the violation occurred;
- Brief description of the events.

Reports may not be used beyond what is necessary to properly follow them up.

All information provided by the Report should be transparent, easy understandable and reliable. This will allow a timely and robust management of the case. For example, information about individual's private life or sensitive data (including health or sex life information) should not be submitted unless it is strictly required or directly relates to the concern. Also, information about individuals that are not connected to the concern raised should be avoided.
Therefore, personal data that are manifestly not useful for processing a specific Report are not collected or, if collected accidentally, are immediately deleted.

The case is assigned to the competent Compliance Officer based on the above information.

The identity of the Reporter(s) and any other information referred to the Report may be disclosed only where it is imposed by European or national law in the context of investigations. Any disclosure of the identity of the Reporter must be managed in strict compliance with local relevant requirements.

The BU/ Group Compliance Officers may be based in a Country other than where the concern took place; however, any information shall be handled in accordance with applicable jurisdictions and this Policy.

The Compliance Officer cannot handle cases involving a subject to whom Compliance Officer reports and cases where Compliance Officer has a potential interest linked to the allegation that could hinder his/her impartiality and independence.

Five steps for managing the Reports

The Reports are managed according to the following steps, which shall be adequately documented:

a) preliminary evaluation;
b) investigation;
c) remedial measures;
d) monitoring;
e) reporting.

a) Preliminary evaluation

As first step, the Compliance Officer undertakes a preliminary evaluation to ensure the appropriate management of the case as follows:

- ensures that he/she has no conflict of interests and the matter falls within her/ his competence and, if not, transmits the Report directly to the competent Compliance Officer within 7 days of receipt;
- acknowledges in writing the receipt of the Concern to the Reporter within seven days of receipt to confirm that the Report has been received and to explain the next steps;
- verifies that the allegation is sufficiently detailed in order to proceed with the evaluation;
- in case of insufficient information, asks the Reporter to provide further information, albeit without there being an obligation to provide such information;
- if the Report turns out not to be sufficiently detailed or no further information is received, dismisses the allegation informing the Reporter;
- if the Report is sufficiently detailed, reports directly and without delay to the Board of Directors, Boards of Auditors and to Surveillance Body the information reported where relevant and proceeds to step b);
- once the preliminary investigations have been completed, the Compliance Officer avails himself of the support of the 231 Corporate Criminal Liability Unit of GBS for the assessments regarding the relevance, pursuant to Legislative Decree 231/01, of the facts exposed in the Report and, if necessary, involves the Surveillance Body.
- Personal data and any information from which the identity of the Reporter, the Facilitators or persons protected by the applicable legislation (i.e. colleagues, family members of the whistleblower) can be inferred must not be communicated to the aforementioned 231 Unit nor to the Surveillance Body.

b) Investigation

Each case is assessed individually.

Once the preliminary evaluation is completed, the relevant Compliance Officer will start investigating the case. He/ she may ask for the support of other functions (e.g., the Human Resources function, Internal Audit function) and/ or of external consultants and counsels (in case of potential criminal liability their involvement is strongly recommended) to verify the legitimacy of the concerns and carry out investigations. In such cases, the relevant Compliance Officer can share with them only the information strictly necessary for the performance of their activities, and the Reporter's identity, where known, only with his/ her explicit consent. Without this consent, no information, fact, or evidence which can allow the Reporter's identification can be shared, unless they have been previously anonymized by the Compliance Officer.

During the investigation, the Compliance Officer examines the circumstances through analysis of documents and data available as well as, if deemed useful, interviewing the Reporter and all other persons considered useful for the resolution of the case and requesting additions from the Reporter.
Investigations must be conducted in a professional way, in compliance with all applicable laws and requirements safeguarding the rights of defense of Persons Concerned.

If the Report has been submitted by telephone hotline or other voice messaging system, the oral Report, subject to the consent of the Reporter, must be documented by:

- making a wiretap of the conversation on a durable medium to allow the information access; or
- doing a complete and accurate transcription of the conversation with the appointed person; this last option must allow the Reporter to verify, amend and approve the call transcription that shall be signed by the Reporter.

If the Reporter asks for a meeting with the Compliance Officer, the meeting must be documented with the prior consent of the Reporter:

- by making a recording of the conversation in a durable and retrievable form; or
- through accurate minutes of the meeting allowing the Reporter to check, rectify and agree by signing them.

During the investigation, all documentation must be stored on a durable medium that allows an easy access to the information, in compliance with the data privacy requirements and for the time necessary to complete the investigation.

When making an interview, the Compliance Officer must consider five credibility assessment factors:

- inherent plausibility;
- demeanour;
- corroboration;
- past record; and
- motive.

The Reporter can follow-up, sending and receiving communications, on the progress of the case. The Compliance Officer diligently updates the Reporter on the status of the case and provides grounded formal responses, which must be the result of an accurate evaluation of the facts.

Investigations must be conducted in a professional and confidential manner, in compliance with all applicable laws and requirements by all parties involved or otherwise aware of the reported matters.

The reporting procedure (from the reporting stage to the informing stage to the Board of Directors) must be completed as quickly as possible according to criteria that consider the seriousness of the violation in order to prevent the continuation of violations from producing further aggravation for the Company. In any case, the procedure must be concluded within 3 months of receipt of the Report.

The Compliance Officer provides feedback to the Reporter within three months from the communication of receipt of the Report or, in the absence of such notice, within three months from the expiry of the term of seven days from the presentation of the Report. Hence, within the same term, any possible investigation on the Person Concerned must have been closed. Indeed, the Person Concerned may be heard, or, at his or her request, shall be heard, also by means of a documentary procedure through the acquisition of written observations and documents.

The Reporter can follow-up, sending and receiving communications to the Compliance Officer in a written way, on the progress of the case.

As a result of the investigation, the Compliance Officer dismisses the Report, if unfounded or unjustified.

The Surveillance Board supervises these activities with reference to reports that are relevant for the purposes of Legislative Decree 231/01, and may at any time provide information, request clarifications and additions to the investigation, and suggest intervention strategies.

c) Remedial measures

If the Report is founded, the Compliance Officer passes the Report to Surveillance Body (where relevant for the purposes of L.D. no. 231/2001) and to the Human Resource. The latter has the duty to:

- identify any remedial measures (of organisational, procedural nature, etc.) to be implemented, in concert with any other relevant function;
- evaluates whether disciplinary sanctions are appropriate, considering local law and internal regulations;
- prepares a comprehensive investigative report;
- submits the proposal for disciplinary sanctions (or other relevant remedial measures) to the Board of Directors/CEO for final decisions.

If the Report is significant, the Surveillance Body proposes the adoption of a disciplinary measure involving the competent structures of the Company.

The investigative report is a document that must be finalized once the investigation is concluded. The report should be detailed in the following sections, as follows:

- Introduction: a summary of the alleged facts and activities performed by the investigators should provide the context allowing to understand the basic elements which have driven the investigation;
- Executive Summary: a short and easy-to-read summary for the facts and analyses should provide a clear picture of the investigation steps and findings, also reassuring that it was handled properly;
- Facts: a clear description of the facts should provide the evidences supporting them including witness statements in a chronological and issues-based narrative form ensuring that the necessary information to assess the case are clearly explained. The facts and evidences should be written with an objective language avoiding any interpretation which could appear biased. Quotes can be used when they have an impact, otherwise it is recommended to paraphrase them (e.g., it is appropriate to paraphrase the offensive language when it is at the center of the issue). Questions asked do not have to be included unless it helps clarify to the answers received.
- Analysis: it should contain credibility determinators such as plausibility, corroboration, motive, history and demeanour to demonstrate well-founded and reasonable conclusions. Everything must be based on the most compelling evidence, including the most relevant information in the document. This implies that the facts and analysis sections can also be merged in order to provide the best representation of the investigation. Moreover, when appropriate it should be a reference to the breach of the law or of the internal regulation, if any.
- Conclusion: brief explanation of what happened and whether it consists in a Breach, thus substantiated or not (or, alternatively, that there was insufficient evidence) and when the case is substantiated, a proposal of remedial and disciplinary measures (only the latter shared with HR function) must be included, detailed and motivated.

Decisions are taken considering that when the Reporter is jointly responsible for the violations, a preferential treatment is given for the latter compared to other jointly responsible persons, compatibly with the applicable regulations.

The Reported Person is protected from negative repercussions deriving from the report in the event that the reporting procedure does not reveal elements that justify the adoption of measures against him. In the event of the adoption of measures against the person responsible for the violation, he must be protected from any negative effects other than those envisaged by the measures adopted.

d) Monitoring

The Compliance Officer, with the support of the Internal Audit Function and the Human Resources, if appropriate, verifies that the approved remedial measures are effectively implemented.

e) Reporting

In addition to the annual reporting to the Board of Directors, the Compliance Officer communicates quarterly to the Group Compliance Officer Function the reports received at local level with the description of each, the current status of their management (even if dismissed), the approved remedial measures (if any) and the status of their implementation. The information must be reported through the case management system Ethics Point.

The remedial measures (when approved by the competent corporate body) must be recorded in accordance with the following classification:
- Communication & Training;
- Policy & Procedures;
- Disciplinary Sanctions, as follows:

  - Informal Warning;
  - Verbal Warning;
  - Written Warning;
  - Demotion;
  - Dismissal.

At least once a year, the Compliance Officer submits to the BoD a report on the allegations received. The Compliance Officer promptly notifies significant Concerns to the Group Compliance Officer, the BoD, the CEO and any other relevant local committee or corporate body.

Feedback to the Reporter(s)
The Reporter(s) must be informed about the action envisaged or taken as follow-up to the Report and the grounds for the choice of that follow-up.

Follow-up could include, for instance, referral to other channels or procedures in the case of reports exclusively affecting individual rights of the Reporter, referral to the appropriate dedicated procedures (e.g., insurance complaints), closure of the procedure based on lack of sufficient evidence or other grounds, launch of an internal enquiry and, possibly, its findings and any measures taken to address the issue raised, referral to a competent authority for further investigation, insofar as such information would not prejudice the internal enquiry or the investigation or affect the rights of the Person Concerned or of any other person involved (including the Compliance Officer(s) and any person(s) supporting the investigation).

The Compliance Officer provides a feedback to the Reporter within three months from the communication of receipt of the Report or, in the absence of such notice, within three months from the expiry of the term of seven days from the presentation of the Report. Hence, within the same term, any possible investigation on the Person Concerned must have been closed. Indeed, the Person Concerned may be heard, or, at his or her request, shall be heard, also by means of a documentary procedure through the acquisition of written observations and documents.

Informing, as far as legally possible and in the most comprehensive way possible, the Reporter(s) about the follow-up to the Report is crucial for building trust in the effectiveness of the Generali Group overall internal system of whistleblower protection and reduces the likelihood of further unnecessary external reports or public disclosures.

6.1 PROTECTION OF DATA AND ARCHIVING

All Reports received and the related documents, via any channels, are stored by the Compliance Officer in the case management system associated to the Helpline as well as in the Group Whistleblowing Case Management System.

Reports are kept and classified as strictly confidential and retained no longer than necessary, until the closure of the case and in accordance with local law on personal data and in accordance with GRE Privacy Policy. The identity of the persons involved and of the persons mentioned in the Report shall be protected until the conclusion of the proceedings initiated as a result of the Report in compliance with the same guarantees provided for in favor of Reporter

Personal information is removed in accordance with the applicable local provisions and only anonymized information is retained to allow reporting and trend analysis.

More in general, personal Data which are manifestly not relevant for the handling of a specific case shall not be collected or, if accidentally collected, shall be deleted without undue delay. The Reports are stored no longer than necessary and proportionate and, in any case, no later than five years from the date of communication of the final outcome of the reporting procedure, in accordance with this Policy, the Directive (EU) 2019/1937 and other European or national obligations.

Circulation of records must be restricted on a “need-to-know” principle and the documentation must be classified, managed and stored in accordance with the Data Governance internal regulations.

The Group Whistleblowing Case Management System allows the production of regular reporting at Local, BU and Group level. Management reporting must be limited to generic details of the cases, such as the number of cases received and grouped by type of allegations involved, geographic areas and measures adopted.

The Reporter and the person concerned are provided with suitable information pursuant to articles 13 and 14 of the Regulation (EU) 2016/679 or article 11 of the Legislative Decree n. 51 of 2018.

7 Anti-Retaliation and Other Protection Measures

7.1 PROHIBITION OF RETALIATION

Retaliation is where someone acts in an unfair or negative way against someone who:

- reports internally or externally in good faith and without gross negligence anonymously or by identifying her/ himself;
- supports another person's Concern;
- collaborates in the investigation of Concerns;
- conducts the investigation.

Although there is no exhaustive list, Retaliation can include (for list of retaliation actions please refer to Annex III):

- employment actions, such as termination, denial of promotion, demotion, job duties change or pay cut;
- other actions affecting employment or having a negative impact such as threats, unjustified negative evaluations, un-justified negative references, increased surveillance or failure to ensure the employees' safety in the workplace;
- harassing and mobbing, including ignoring and avoiding the Employee in an obvious manner, failing to provide the Employee with important information needed to perform his/her job or blaming the Employee for causing problems because he/she filed a concern or remarking that the Employees should transfer or quit the job;
- physical harm which can manifest itself in a verbal, physical or written form.

The Generali Group is committed to maintain a work environment free of harassment, intimidation, discrimination and Retaliation for engaging in protected activities such as reporting violations or participating in an investigation pertaining to alleged violations of the law, the Code or other internal regulation. Crucial to these objectives is promoting an environment where Employees and others feel safe to engage in frank and honest communication, raising questions or Concerns at any time without fear of Retaliation.

The Company strictly prohibits any form of retaliatory action against Employees who raise issues or ask questions, report a Concern, participate in an investigation, refuse to participate in suspected improper or wrongful activity.

Retaliation is egregious misconduct. Any form of Retaliation, including vexatious, will be subject to penalties up to employment termination. Generali Group shields the Employee against Retaliation even if the Concerns raised in good faith and without gross negligence are not confirmed following an investigation.

Any person who makes an external reporting to competent authorities or a public disclosure must be protected by the Group and by the Company:

- if he/ she has reported internally but no appropriate action was taken in response to the report within the timeframe established by this Policy or by local requirements;
- if this disclosure has been done in good faith and without gross negligence and if the reported Breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency or a risk of irreversible damage;
- when it is required by the local laws.

The Company must consider that in legal proceedings, including for defamation, breach of copyright, breach of secrecy, breach of data protection rules, disclosure of trade secrets, or for compensation claims based on private, public, or on collective labor law, the Reporters do not incur liability of any kind as a result of reports or public disclosures under the EU Directive. Those Reporters have the right to rely on that reporting or public disclosure to seek dismissal of the case, provided that they had reasonable grounds to believe that the reporting or public disclosure was necessary for revealing a breach, pursuant to the EU Directive.
However, this anti-retaliation provision does not exempt Employees from the consequences of their own misconduct such as knowingly making false allegation, illegally access to information, provide false or misleading information during an investigation or act in bad faith. Any abuse of the process by the Reporter to obtain a personal advantage or simply to slander or libel the reported person are not tolerated.

CEOs ensure that Employees are protected against any form of Retaliation.

The Compliance Officer shall put in place proper monitoring and controls during and after the investigation so to protect the relevant persons from retaliation actions. To this aim, the Compliance Officer schedules at least a meeting with the Reporter(s) potentially exposed to any form of Retaliation during the first six months after the closing of the case. The Reporter(s) are always and strongly encouraged to timely contact the Local or Group Compliance Officer to inform about any occurred or potential future retaliatory action without any fear of reprisal.

When the Compliance Officer envisages a risk of retaliation, he/ she has to notify the risk to the Local HR Function. This latter must inform the Local Compliance Officer in advance and with written communications about any disciplinary measure in order to prevent retaliation actions.

7.2 OTHER PROTECTION MEASURES

In addition to the prohibition of retaliation, Decree 24 establishes additional protection measures, described in the paragraphs below.

All the protection measures, including the prohibition of retaliation, also apply to:

a) Facilitators;
b) persons in the same employment context as the Reporter or the person who made a judicial or accounting report or made a public disclosure and who are bound to them by a stable emotional or family relationship up to the fourth degree;
c) co-workers of the Reporter or of the person who made a report to the judicial or accounting authority or made a public disclosure, who work in the same work environment as the reporting person and who have a regular and current relationship with that person;
d) entities owned by the Reporter or by the person who made a complaint to the judicial or accounting authorities or who made a public disclosure or for whom the same persons work, as well as entities working in the same work environment as the said persons.

as well as in case the reporting, complaint to the judicial or accounting authority or public disclosure of information occur in the following cases:

e) when the legal relationship referred to in Article 3 paragraph 3 of Decree 24 has not yet begun, if the information on the violations has been acquired during the selection process or in other pre-contractual phases;
f) during the trial period;
g) after the dissolution of the legal relationship if the information on the violations was acquired during the relationship itself.

Furthermore, such protection measures apply to Reporters when they use an internal or an external reporting channel or make a public disclosure or a complaint to the judicial or accounting authority, provided that the following conditions are met:

A. at the time of reporting or reporting to the judicial or accounting authorities or of public disclosure, the reporting or complaining person had reasonable grounds to believe that the information on the reported, publicly disclosed or reported violations was true and fell within the objective scope of referred to in article 1 of Decree 24;
B. the reporting or public disclosure was made in compliance with the indications of Decree 24 indicated in this Policy.

The reasons that led the person to make Report, to report to judicial or accounting authorities or to publicly disclose are irrelevant to such protection.

When the criminal liability of the reporting person for defamation or slander crimes or in any case for the same crimes committed with the report to the judicial or accounting authority or its civil liability, for the same title, in cases of willful misconduct or gross negligence, all protection measures established by L.D. No. 24/2023, are not guaranteed and a disciplinary sanction is imposed on the reporting or reporting person (see paragraph 2.1).

Such provisions also apply in cases of Report or reporting to the judicial or accounting authority or anonymous public disclosure, if the Reporter was subsequently identified and suffered retaliation, as well as in cases of reporting presented to institutions, to the competent bodies, offices and agencies of the European Union, in accordance with the conditions set out in Article 6 of L.D. No. 24/2023.

Liability Constraints

Decree 24 establishes the *non-punishment* of the Company or the person who discloses or disseminates information on violations covered by the obligation of secrecy (other than classified information; forensic and medical professional secrecy; secrecy of the deliberations of the courts) or relating to the protection of copyright or the protection of personal data or reveal or disseminate information on violations that offend the reputation of the person involved or reported when:

- at the time of the disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of the same information was necessary to reveal the violation and
- the reporting, public disclosure or complaint to the judicial or accounting authority was made pursuant to requirements set out by L.D. no. 24/2023 and described in the paragraphs above.

In this case, any further liability, even of a civil or administrative nature, is also excluded.

Unless the fact constitutes a crime, the subjects above do not incur any liability, even of a civil or administrative nature, for the acquisition of information on the violations or for access to them.

In any case, criminal liability and any other liability, including of a civil or administrative nature, is not excluded for behaviors, acts or omissions not related to Report, reporting to the judicial or accounting authority or public disclosure, or which they are not strictly necessary to reveal the violation.

Waivers and Transactions

The waivers and transactions, in whole or in part, which have as their object the rights and protections provided for by this decree are not valid, unless they are carried out in the forms and ways referred to in article 2113 fourth paragraph of the Italian civil code (i.e, the above does not apply to waivers and transactions signed in protected venues - judicial, union administration).
Therefore, the whistleblower and the other protected subjects can validly renounce their rights and means of protection or make them the subject of a settlement, if this takes place before a judge, following a mandatory attempt at conciliation or mediation and conciliation agreements prepared by unions.

Support Measures

The ANAC provides the whistleblower with support measures which consist of free information, assistance and consultancy (please refer to the ANAC website).

ANNEX I– CATEGORIES OF ISSUE TYPES

Anyone (e.g., current or past Employees, candidates, vendors, consultants, other stakeholders) who has reported or witnessed a Breach may report a Concern.
Concerns reported are classified according to the Issue Types in the following table.
This classification is also aimed at helping the Reporter in understanding if some bad practices are being performed or were performed in the past and that they must be reported to reinforce and protect the integrity of the work environment and avoid direct losses and reputational impacts for the single Group Legal Entity and the entire Group.

Issue Types	Description
Antitrust	- Top Management, to eliminate competition, deprive smaller competitors of customers by selling at artificially low prices they can't compete with; - The Company uses its dominant position directly or indirectly to impose unfair purchase or selling prices or other unfair contractual conditions - The Company makes the sale of one product conditional on the sale of another product to limit market competition.
Assets and Business Data Protection	- Employees misuse undertaking's equipment, materials or premises; - Employees disclose confidential information, financial data or documents; - No protection of intellectual property with patents, trademarks and copyright.
Bribery and Corruption	- Accepting undue payments, gifts, entertainment, or other benefits from business partners (i.e., suppliers, intermediaries, consultants, and any other persons working with or for Generali); - Promising or giving money, gifts, entertainment or other benefits to public officials, customers, or business partners; - Performing incomplete due diligence on customers or business partners (e.g., information is not collected regarding historic allegations for bribery and corruption, involvement of a public official in a high-risk country is not detected, verification of existence of a business partner); - Ignoring red flags indicators (e.g., request to change payment recipient, request of international payment, refusal of providing information) when performing due diligence controls for relevant areas of risk (e.g., procurement, underwriting, sells).
Business Continuity	- No business continuity policy; - The business contingency plans are not periodically reviewed and/or tested; - Relevant company management and personnel have not been informed about the business contingency plans.

Issue Types	Description
Capital Management	- No medium-term capital management plan that assures adequate capitalization for the strategic objectives; - Missing development of procedures aimed at ensuring that own funds item, terms and conditions are clear and unmistakable; - No forward-looking approach for capital management planning; - No analysis on legal, risk, accounting, tax and regulatory aspects before executing other risk mitigation techniques.
Conflict of interests	- An employee does not disclose a situation that may impair or be perceived to impair its ability to act with integrity and impartiality; - An employee performs an external paid activity that is in potential competition with the business of the undertaking, without obtaining prior approval; - Appropriate remedial measures for the specific conflict case have not been adopted (i.e.: removing the Employee from all decisions involving the conflict of interest).
Customer Relationship	- Complaints, surrenders and any other contractual obligation are not managed within the time prescribed by local regulations, registered in a databank, and handled by a specific business function; - Policyholders are not provided with the ongoing information/documentation (e.g., reports on the service provided, periodic communications and periodic assessment of suitability, if any).
Discrimination, Harassment and Retaliation	- Unfair treatment or arbitrary distinction based on a person's age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation, ethnic or social origin or other status; - Employees harass, mob or bully colleagues for example with sexually oriented e-mails or text messages, unwelcome gestures, or physical contact, offensive or degrading comments about personal characteristics, as well as using inappropriate language; - The reporter is subject to retaliation (punishment due to his/her report) for example through: termination, denial of promotion, demotion, job duties change or pay cut, unjustified negative evaluations, blaming the employee for causing problems because he/she filed a concern.
Distribution	- The insurance products are sold through unauthorized intermediaries; - The distributor does not ask for information on the policyholder's personal characteristics, with special regard to his/her age, employment, family, financial

Issue Types	Description
	and insurance position, risk propensity and expectations from the contract in terms of coverage, duration, ESG (Environmental, Social and Governance) preferences and any financial risks related to the contract to be concluded; - Investment: not adequate retrieval of information in relation to client/subscriber personal characteristics, employment, family, financial position, risk tolerance and expectations from the contract in terms of coverage, ESG (Environmental, Social and Governance) impact, duration and any financial risks related to the contract to be concluded.
Ethical and Sustainable Culture	- Unethical behaviours are identified but permitted or tolerated by Top Management; - An employee of the undertaking adopts a dishonest and unethical behaviour in the performance of the working activity (i.e.: an employee has been seen steeling a wallet from a colleague's handbag); - Skills and resources of the Group are not put at the service of those who are most vulnerable, to promote the integration of the poorest and most disadvantaged people; - No protection of the environment neither promotion of a reduction in the direct and indirect environmental impact of the Company's activities.
External Fraud	- Events arising due to fraud, robbery or misappropriation perpetrated by intermediaries against the customers; - An intermediary lodge the payment for a new policy or of a claim or surrender into his/her bank account.
Financial Reporting	- The Company does not include a reliable analysis of the business outlook and operating results in its annual report; - The Company drafts an annual report not complying with the local accounting standards.
HR Administration	- Improper employee administration concerning wage and hour law (minimum wage and number of work hour per week); - The employee benefits are not guarantee (care law, retirement, health insurance programs); - The employee rights are not guarantee (pregnancy covering); - The mandatory reporting concerning the employees are not respected (personnel income tax, communication to the labour office.
Internal fraud – Administrative Personnel	- Events arising due to intentional acts – other than the ones already covered by other compliance risks (e.g.: bribery and corruption) - illegally performed by

Issue Types	Description
	administrative staff, to obtain a profit for themselves or for others, resulting in a damage for the Company; - Robberies, petty thefts towards the company or colleagues, forged signature, falsification of invoices and documents with the intent to defraud the Company.
Internal fraud - Intermediaries	- Events arising due to intentional acts – other than the ones already covered by other compliance risks (e.g.: bribery and corruption) - illegally performed by intermediaries/sales personnel, to obtain a profit for themselves or for others, resulting in a damage for the Company. - Actions aimed at obtaining undue commissions and payments from the Company.
International Sanctions	- Working with international customers in high risks sectors (e.g., oil & gas, gambling, energy, defence) and/or in high areas (e.g., Middle East, Russia, Far East, Central America); - Providing, directly or indirectly, any financial services (e.g., insurance coverage, receiving or processing a payment) to parties included in UN, EU, US, or local sanctions lists; - Missing or weak implementation of a screening tool to detect sanctioned individuals; - Misunderstanding of the applicable requirements due to lack of training and/or knowledge of Group Internal Regulations.
IT Systems and Security	- No definition of a strategic plan on information and communication technology; - No adequate implementation of procedure for ensuring secure access to the IT environments.
Market Abuse	Market Abuses may consist in: - insider dealing; - recommendation of, or inducement to, engaging or attempting to engage in insider dealing; - unlawful disclosure of inside information; or market manipulation.
Marketing & Advertising	- Risk is associated with failure to advertise products as prescribed by laws and regulations; - The advertising is not immediately and clearly recognizable as such; - Marketing communications and advertisements discredit or denigrate another product, marketer, trademark, trade name or other distinguishing mark.
Money Laundering	- Failing to properly evaluate the money laundering risk profile of a customer;

Issue Types	Description
	- Performing inadequate customer due diligence during the onboarding of a new customer; - Missing the identification of all relevant parties of a business relationship; - Ignoring red flags and anomalous behaviours which could led to not reporting a suspicious transaction; - Missing appointment of persons responsible for anti-money laundering compliance (i.e., AML Officer and Money Laundering Reporting Officer).
Other	Any other case that cannot be classified under the Risks catalogue definitions and the further ones provided
Personal Data Protection	- Personal data is transferred to external providers/group companies, outside the European Union without a valid safeguard (e.g., to a not adequate Country); - The data subject is not informed about how personal data collected will be used and who will have access to it; - Personal data are stored without having pre-defined a proper storage period (e.g., in compliance with local applicable laws).
Related Party Transactions	- No written procedure on how Related Party Transactions should be managed; - Missing list of Related Parties; - The undertaking does not adopt the necessary procedures (e.g., identification of the transactions, identification of the manner whereby related party transactions are executed and approved) to ensure transparency and substantial and procedural fairness of Related Party transactions.
Remuneration	- The remuneration package of key personnel is not aligned with the level of responsibility and the commitment relating to the role; - Key personnel is not remunerated respecting a sound and prudent risk management or its strategic objectives, profitability and balance in the long run; - Payment policies are based exclusively or mainly on short-term performance and/or on financial objectives; - Disrespected regulatory prescriptions in defining the remunerations of directors, internal control functions, etc., (e.g., balance between fixed and variable components, performance setting and measurement, payment of the variable component, remuneration based on financial instruments, sums paid in case of early termination of the appointment); - The implementation of remuneration policy is not verified by the internal control functions.
System of Governance	- The system of governance, the internal control and risk management system are not effective and well-

Issue Types	Description
	integrated into the organizational structure and in the decision-making processes; - The AMSB has not been established in the Group Legal Entities; - The structure of the system of governance is not documented; - No formalized procedure for assessing the fitness and integrity of the persons who effectively run the undertaking or have other key functions; - No identification of the key personnel and no verification of the fit and proper requirements of the persons who run the undertaking or have other key functions; - The key personnel fail to communicate a circumstance that leads to the loss of their proper requirements; - Outsourcing agreements are not formalized in writing or do not include the proper SLAs to monitor service quality; - The undertaking does not appoint a person responsible for supervising over outsourced functions; - The undertaking does not set up specific monitoring and controlling processes to govern risks derived from outsourcing functions and/or activities and to monitor related performances; - The undertaking does not set up proper contingency plans to ensure the continuity of the activities (i.e., exit strategy) in case of an interruption or severe deterioration in the quality of the service provided.
Tax	- Unpaid tax on the mathematical provisions of life policies in compliance with local tax provisions pro tempore in force.
Tax Avoidance and Evasion	- Selling FATCA relevant products without performing the correct client identification and classification processes to avoid that this is sold to an U.S. person; - Missing implementations of Group Standards to comply with the FATCA and CRS requirements (i.e., Group FATCA & CRS Compliance Programs is not implemented); - No list of product classifications maintained to understand which customers are subjected to FATCA & CRS requirements; - Missing appointment of a person responsible for tax avoidance and evasion (e.g., FATCA Responsible Officer).
Terrorist Financing	- Performing inadequate customer due diligence during the onboarding of a new customer; - Accepting and/or executing payments on behalf and/or towards persons on the terrorist lists (including UN, EU, OFAC and local lists);

Issue Types	Description
	- Missing implementation of screening processes to ensure detections of terrorists and freezing of funds; - Ignoring red flags and anomalous behaviours which could led to not reporting a suspicious transaction; - Missing screening of all relevant parties of a business relationship; - Missing appointment of persons responsible for counter-terrorism financing compliance (i.e., Compliance Officer or AML Officer and Money Laundering Reporting Officer).
Whistleblowing	- Whistleblowing channels to report unethical or incorrect behaviours are not set up and communicated to employees; - Whistleblowing channels in line with local regulation are not ensured, neither appropriate communication nor training are provided to employees; - Appropriate remedial measures are not implemented (e.g., issue of internal regulation, training, disciplinary measures).
Workspace Security	- A safe and healthy working environment is not provided; - Employees do not respect the security measures which may endanger health and safety of themselves and/or others; - Employees don't minimize the environmental impact of their working activities.

ANNEX II – PROHIBITED RETALIATORY PRACTICES

The Company takes the necessary measures to prohibit any form or retaliation against a Reporter (e.g., current or past Employees, candidates, vendors, consultants, other stakeholders), including for example threats of retaliation and attempts of retaliation in the form of:

a) suspension, lay-off, dismissal or equivalent measures;

b) demotion or withholding of promotion;

c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;

d) withholding of training;

e) a negative performance assessment or employment reference;

f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;

g) coercion, intimidation, harassment or ostracism;

h) discrimination, disadvantageous or unfair treatment;

i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;

j) failure to renew, or early termination of, a temporary employment contract;

k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;

l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;

m) early termination or cancellation of a contract for goods or services;

n) cancellation of a licence or permits;

o) psychiatric or medical referrals.