



## **Policy sul sistema di segnalazione delle condotte illecite (Policy di *Whistleblowing*)**

---

PY071-003

Approvazione  
07/11/2025

Efficacia  
10/11/2025

**INDICE**

<b>1. INTRODUZIONE.....</b>	<b>4</b>
1.1. OGGETTO E OBIETTIVI DELLA POLICY .....	4
<b>2. RUOLI E RESPONSABILITÀ.....</b>	<b>5</b>
<b>3. PRINCIPI E LINEE GUIDA .....</b>	<b>6</b>
3.1. SOGGETTI BENEFICIARI DEL SISTEMA DI SEGNALAZIONE .....	6
3.2. FATTISPECIE OGGETTO DI SEGNALAZIONE ED ESCLUSIONI .....	6
3.3. MODALITA' DI SEGNALAZIONE DELLE VIOLAZIONI .....	7
3.4. COMPILAZIONE DELLA SEGNALAZIONE .....	8
3.5. ASSEGNAZIONE INIZIALE DELLA SEGNALAZIONE ED ESCALATION .....	9
3.6. ESAME E VALUTAZIONE PRELIMINARE DELLE SEGNALAZIONI .....	9
3.7. INDAGINI E COMUNICAZIONE ESITO .....	9
3.8. DEFINIZIONE DELLE MISURE CORRETTIVE .....	11
3.9. PROVVEDIMENTI DECISIONALI .....	11
3.10. MONITORAGGIO.....	12
3.11. MISURE DI PROTEZIONE E ANTI-RITORSIONE .....	12
3.12. OBBLIGHI INFORMATIVI E REPORTING.....	13
<b>4. GESTIONE DELLA POLICY E RIFERIMENTI NORMATIVI .....</b>	<b>14</b>
4.1. GESTIONE DEL DOCUMENTO .....	14
4.2. RIFERIMENTI NORMATIVI.....	14
4.3. PERIMETRO DI APPLICAZIONE .....	15
<b>5. GLOSSARIO .....</b>	<b>16</b>

**STORICO DELLE VERSIONI**

<b>Versione</b>	<b>Data di approvazione</b>	<b>Descrizione sintetica delle modifiche</b>	<b>Normativa abrogata / sostituita</b>
<b>001</b>	22/06/2023	<i>La Policy disciplina gli aspetti di natura organizzativa e procedurale dei sistemi interni di segnalazione</i>	<i>Procedura di gestione delle segnalazioni interne di violazione delle norme disciplinanti l'attività</i>

		<i>delle violazioni (c.d. "whistleblowing")</i>	<i>bancaria (Procedura di Whistleblowing)</i>
<b>002</b>	24/10/2024	<i>Aggiornamento della disciplina dei soggetti designati ai fini dell'assegnazione iniziale delle segnalazioni e delle regole di escalation</i>	-
<b>003</b>	10/11/2025	<i>Aggiornamento a seguito modifiche della struttura organizzativa</i>	.
<b>POLICY OWNER</b>			
<b>Responsabile Chief Compliance Office</b>			

## 1. INTRODUZIONE

I legislatori europeo ed italiano hanno introdotto i sistemi di segnalazione interna delle violazioni alla normativa, conosciuti anche come sistemi di whistleblowing.

Tali sistemi sono istituiti per consentire la segnalazione di violazioni della normativa di cui si venga a conoscenza nel contesto lavorativo al fine di favorire la diffusione di condotte eticamente conformi e la tutela della legalità.

Il quadro normativo in materia disciplina gli aspetti di natura organizzativa e procedurale dei sistemi interni di segnalazione delle violazioni (c.d. "whistleblowing") che le banche devono adottare. Detta disciplina si fonda su due principi rilevanti:

- la tutela del soggetto segnalante e di altri soggetti contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
- la garanzia della riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione.

### 1.1. OGGETTO E OBIETTIVI DELLA POLICY

Banca Generali, in linea con i principi che ispirano il Gruppo Generali, promuove e favorisce la diffusione di una cultura aziendale della legalità caratterizzata da comportamenti corretti e garantisce efficaci ed efficienti mezzi volti a prevenire, gestire ed eventualmente segnalare internamente eventuali irregolarità o violazioni delle norme disciplinanti l'attività aziendale, attraverso canali sicuri e riservati. A tal riguardo, la Banca richiede ai propri Collaboratori nello svolgimento delle loro mansioni, il rispetto dei più elevati standard di onestà ed integrità nonché di salvaguardare le risorse di cui ciascuno è responsabile.

Banca Generali adotta il presente documento al fine di disciplinare i criteri e le regole che consentono di gestire le segnalazioni che il personale può effettuare, in relazione a fenomeni fraudolenti e comportamenti sospetti, nonché a irregolarità nella conduzione aziendale o violazione delle norme disciplinanti l'attività.

In particolare, il documento ha l'obiettivo di definire:

- gli organi e le funzioni coinvolte nella gestione delle segnalazioni, descrivendo i relativi ruoli e responsabilità;
- i canali posti a disposizione del segnalante volti a denunciare presunte anomalie o violazioni effettuate da dipendenti, membri degli organi sociali o terzi;
- il perimetro oggettivo e il contenuto della segnalazione;
- i soggetti beneficiari dei sistemi di segnalazione (i segnalanti) e le forme di tutela previste nei confronti degli stessi;
- le modalità di gestione della segnalazione e del suo stato di avanzamento;
- le modalità di conservazione dei documenti.

La presente Policy, al fine di garantirne la diffusione, è pubblicata sul sito istituzionale della Banca e sull'intranet aziendale.

## 2. Ruoli e Responsabilità

Organo / funzione	Responsabilità
<b>Chief People Office</b>	<ul style="list-style-type: none"><li>decide sui provvedimenti di competenza da emettere nei confronti del personale coinvolto nelle violazioni, in qualità di struttura deputata ad eseguire i provvedimenti disciplinari del personale dipendente secondo quanto previsto dai poteri delegati dal Consiglio di Amministrazione e/o dall'Amministratore Delegato e Direttore Generale.</li></ul>
<b>Chief Compliance Office</b>	<ul style="list-style-type: none"><li>il Responsabile è identificato quale <i>Responsabile dei sistemi interni di segnalazione</i>, assicura il corretto svolgimento del procedimento di trattazione delle segnalazioni, la gestione conforme del sistema di segnalazione e le connesse attività di reporting verso gli organi sociali..</li></ul>
<b>Chief Audit Office</b>	<ul style="list-style-type: none"><li>il Responsabile collabora con il <i>Responsabile dei sistemi interni di segnalazione</i>, ove da quest'ultimo richiesto ai sensi del successivo par. 3.7 in funzione dell'oggetto e tipologia della segnalazione, nelle attività di valutazione ed indagine conseguenti; è altresì identificato quale destinatario alternativo delle segnalazioni nei casi previsti dalla Policy.</li></ul>
<b>Amministratore Delegato e Direttore Generale</b>	<ul style="list-style-type: none"><li>decide sui provvedimenti di competenza da emettere nei confronti del personale dipendente coinvolti nelle violazioni secondo quanto previsto dai poteri delegati dal Consiglio di Amministrazione.</li></ul>
<b>Comitato Nomine e Governance</b>	<ul style="list-style-type: none"><li>Il Presidente del Comitato Nomine e <i>Governance</i> gestisce, con l'eventuale supporto di altre strutture aziendali e/o consulenti tecnici, le segnalazioni riguardanti il Presidente del Consiglio di Amministrazione.</li></ul>
<b>Consiglio di Amministrazione</b>	<ul style="list-style-type: none"><li>approva la relazione annuale sul corretto funzionamento dei sistemi interni di segnalazione delle violazioni;</li><li>è informato sulle violazioni di particolare gravità unitamente all'Amministratore Delegato e al Collegio Sindacale. Il Presidente del Consiglio di Amministrazione gestisce, con l'eventuale supporto di altre strutture aziendali e/o consulenti tecnici, le segnalazioni riguardanti l'Amministratore Delegato o un membro del Consiglio di Amministrazione.</li></ul>

### 3. PRINCIPI E LINEE GUIDA

#### 3.1. SOGGETTI BENEFICIARI DEL SISTEMA DI SEGNALAZIONE

Ai sensi della vigente normativa, le segnalazioni possono essere effettuate dalle seguenti persone che prestano la loro attività lavorativa o intrattengono rapporti con la Banca o il Gruppo Bancario:

- i lavoratori dipendenti (qualunque tipologia contrattuale), gli stageur;
- i consulenti finanziari;
- i soggetti terzi che intrattengono rapporti e relazioni d'affari durevoli con la Banca o con il gruppo bancario (e.g. collaborazioni coordinate e continuative, consulenti stabilmente inseriti in azienda sulla base di rapporti time material, etc.);
- i fornitori di beni e servizi;
- le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza;
- gli azionisti.

Le segnalazioni sono ammesse anche:

- quando il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali (ad es. candidati);
- successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite prima dello scioglimento del rapporto stesso (e.g. pensionati).

#### 3.2. FATTISPECIE OGGETTO DI SEGNALAZIONE ED ESCLUSIONI

I soggetti beneficiari (i segnalanti) possono segnalare comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità di Banca Generali o del Gruppo Bancario e che possano costituire in particolare:

- una violazione delle norme disciplinanti l'attività bancaria, l'intermediazione finanziaria e la distribuzione di prodotti assicurativi;
- una violazione potenziale o effettiva delle disposizioni in materia di prevenzione del riciclaggio e del finanziamento del terrorismo;
- una grave irregolarità o violazione della normativa applicabile alla Banca e al gruppo bancario come di seguito specificato.

Le segnalazioni dovrebbero pertanto riguardare circostanze e condotte negligenti, illecite, irregolari o non corrette riguardanti l'attività lavorativa, per cui vi è il ragionevole sospetto o delle quali si è venuti a conoscenza nello svolgimento delle proprie funzioni, a titolo esemplificativo e non esaustivo in relazione a:

- irregolarità amministrative e negli adempimenti contabili e fiscali;
- irregolarità in materia di antiriciclaggio e contrasto finanziario al terrorismo;
- irregolarità in materia di *market abuse* e altre irregolarità nella prestazione dei servizi e attività di investimento;
- irregolarità in materia di distribuzione di prodotti assicurativi;
- violazioni della disciplina sulla riservatezza dei dati;

- violazioni del codice interno di comportamento;
- violazioni del Modello di organizzazione e gestione ex d.lgs. 231/2001;
- violazione della normativa in materia di usura;
- bullismo e molestie;
- corruzione;
- appropriazioni indebite e malversazioni (monetarie e relative a beni materiali ed immateriali);
- frodi;
- illeciti riguardanti l'operatività bancaria di erogazione del credito (es. trasparenza, etc.);
- illecito esercizio delle deleghe attribuite;
- altre fattispecie che possono costituire violazione delle norme disciplinanti l'attività bancaria.

Sono esclusi dalla disciplina in esame tutti quegli atti o fatti che si riferiscono, a titolo esemplificativo e non esaustivo, a:

- richieste della clientela;
- operazioni sospette ai sensi del D. Lgs 231/2007 e successive modifiche e integrazioni per le quali deve essere attivata la specifica procedura prevista dalla normativa interna;
- informazioni già di dominio pubblico (ad esempio: articoli di giornale, rapporti pubblici di audit, ecc.);
- reclami di carattere personale del segnalante, rivendicazioni/istanze che rientrano nella disciplina del rapporto di lavoro o lamentele legate ai rapporti col superiore gerarchico o colleghi;
- rischi immediati per la vita o per la proprietà (in questi casi è necessario attivare le altre procedure previste come, a titolo esemplificativo, il piano antincendio, il piano di continuità operativa ovvero chiamare i numeri nazionali di emergenza);
- voci non confermate/dicerie.

Le segnalazioni possono riguardare:

- dipendenti e dirigenti di ogni ordine e grado;
- membri degli organi sociali;
- terzi collegati ai soggetti sopra citati (fornitori, consulenti).

### **3.3. MODALITA' DI SEGNALAZIONE DELLE VIOLAZIONI**

Ferma restando la possibilità per il personale di rivolgersi al proprio responsabile/manager diretto per eventuali dubbi o preoccupazioni, i soggetti (come definiti al par. 3.1.) che rilevino atti o comportamenti che, in buona fede, considerino in violazione delle norme possono trasmettere una segnalazione utilizzando i seguenti canali:

1. tramite la piattaforma informatica disponibile sui siti societari, telefonicamente o via web;
2. tramite posta elettronica alla casella mail appositamente costituita ([segnalazioni.whistleblowing@bancagenerali.it](mailto:segnalazioni.whistleblowing@bancagenerali.it));
3. per iscritto in busta riservata e personale inviata al "Responsabile di Chief Compliance Office";

4. chiedendo, con sufficiente preavviso, un incontro al “*Responsabile di Chief Compliance Office*”.

Si evidenzia che la piattaforma consente di indicare se la segnalazione riguarda il Responsabile di *Chief Compliance Office* affinché la relativa valutazione sia effettuata in assenza di conflitti di interesse dal Responsabile di *Chief Audit Office*.

I Segnalanti possono decidere di segnalare in forma anonima. In questo caso, la piattaforma informatica dedicata fornisce un codice identificativo per consentire lo scambio di informazioni con il *Responsabile dei sistemi interni di segnalazione*.

Sebbene le segnalazioni anonime siano accettate, il Gruppo bancario incoraggia a rivelare l'identità durante la presentazione di una segnalazione, poiché ciò di solito consente un'indagine più efficace. Al fine di facilitare la divulgazione, il Gruppo bancario ha stabilito specifiche misure di protezione contro eventuali azioni di ritorsione.

Il Segnalante ha inoltre l'obbligo di dichiarare se ha un interesse privato collegato alla segnalazione. Le segnalazioni devono essere circostanziate, ragionevoli e significative e non possono essere basate su un pregiudizio o preconcetto.

Dovrebbero contenere i dettagli necessari per consentire un'indagine. Le segnalazioni prive di informazioni sufficienti non permettono di avviare un'indagine e richiedono pertanto di essere approfondite con la collaborazione del segnalante al fine di raccogliere le informazioni sufficienti per fondare un'indagine.

I Segnalanti sono tenuti a raccogliere e organizzare le informazioni pertinenti al fine di facilitare l'indagine interna fornendo un quadro chiaro e sufficiente per supportare la comprensione del caso e consentire un'indagine imparziale ed equa da parte della funzione competente.

### **3.4. COMPILAZIONE DELLA SEGNALAZIONE**

Di seguito si forniscono alcune indicazioni per una corretta compilazione della segnalazione, valide per qualsiasi canale sia prescelto dal segnalante, in particolare nel caso in cui non venga utilizzata la piattaforma informatica dedicata che comporta la compilazione dell'apposito *form*.

La segnalazione dovrebbe prevedere almeno l'indicazione delle seguenti informazioni:

1. Società e struttura aziendale a cui si riferisce la segnalazione;
2. eventuale presenza di un interesse privato collegato alla segnalazione;
3. tipologia di violazione;
4. descrizione dei fatti oggetto di segnalazione;
5. data o periodo in cui sono avvenuti i fatti segnalati;
6. modalità con cui si è venuti a conoscenza dei fatti segnalati;
7. soggetti e funzioni aziendali coinvolte nei fatti segnalati.

La segnalazione può inoltre contenere le seguenti informazioni utili alle indagini:

8. eventuali beneficiari dei fatti segnalati;
9. eventuali soggetti danneggiati dai fatti segnalati;
10. eventuale valore economico dei fatti segnalati;
11. eventuali terzi coinvolti nei fatti segnalati (fornitori, clienti, ecc.);
12. eventuali informazioni utili per verificare la veridicità della segnalazione;

13. ogni altra informazione utile.

La segnalazione può inoltre essere corredata da eventuale documentazione a supporto.

### **3.5. ASSEGNAZIONE INIZIALE DELLA SEGNALAZIONE ED ESCALATION**

La segnalazione viene assegnata al *Responsabile dei sistemi interni di segnalazione* e gestita dallo stesso nel rispetto di quanto indicato ai paragrafi successivi, fatti salvi i seguenti casi che sono gestiti secondo le seguenti regole di *escalation* a garanzia dell'imparzialità e indipendenza di giudizio:

- segnalazioni riguardanti il Responsabile dei sistemi interni di segnalazione che sono assegnate e gestite dal Responsabile di *Chief Audit Office*;
- segnalazioni riguardanti l'Amministratore Delegato o un membro del Consiglio di Amministrazione che sono assegnate e gestite dal Presidente del Consiglio di Amministrazione;
- segnalazioni riguardanti il Presidente del Consiglio di Amministrazione che sono assegnate e gestite dal Presidente del Comitato Nomine e *Governance*.

### **3.6. ESAME E VALUTAZIONE PRELIMINARE DELLE SEGNALAZIONI**

Il *Responsabile dei sistemi interni di segnalazione* effettua una valutazione preliminare per garantire la gestione appropriata del caso come segue:

1. assicura che non vi siano conflitti di interesse e che la questione rientri nelle sue competenze e, in caso contrario, trasmette la segnalazione direttamente al soggetto competente;
2. rilascia avviso per iscritto del ricevimento della segnalazione entro sette giorni dal ricevimento stesso;
3. verifica che la segnalazione sia sufficientemente dettagliata per poter procedere alla valutazione;
4. in caso di informazioni insufficienti, chiede al Segnalante di fornire ulteriori informazioni, senza tuttavia che vi sia l'obbligo di fornire tali informazioni;
5. se la segnalazione risulta non sufficientemente dettagliata e non sono state ricevute ulteriori informazioni, l'archivia dandone comunicazione al Segnalante;
6. se la segnalazione è sufficientemente dettagliata, procede con l'attività di indagine.

Analogo procedimento viene applicato dal Responsabile di *Chief Audit Office* o da altri soggetti quando chiamati alla trattazione della segnalazione ai sensi del paragrafo 3.5.

### **3.7. INDAGINI E COMUNICAZIONE ESITO**

Una volta completata la valutazione preliminare, il *Responsabile dei sistemi interni di segnalazione* avvia le indagini sul caso.

Le indagini devono avere una durata ragionevole e sono eseguite da *Chief Compliance Office* e/o da *Chief Audit Office* a seconda della tipologia di segnalazione e dei rispettivi ambiti di competenza che opereranno in maniera indipendente e secondo propri approcci e finalità standard e si potranno avvalere del supporto di altre strutture aziendali e/o consulenti tecnici (quali, ad esempio, studi legali esterni o specialisti interni alla Banca) su materie che non rientrano nella propria specifica competenza.

Per le segnalazioni relative a presunte violazioni della normativa antiriciclaggio, sarà il Responsabile della funzione antiriciclaggio ad effettuare gli accertamenti del caso ed eventualmente effettuare le comunicazioni previste dal D.Lgs. 21 novembre 2007 n. 231.

In tali casi, il *Responsabile dei sistemi interni di segnalazione* può condividere con il Segnalante solo le informazioni strettamente necessarie allo svolgimento delle proprie attività, e l'identità del Segnalante, ove nota, solo con il suo esplicito consenso a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare i dati. Senza questo consenso, nessuna informazione, fatto o prova che possa consentire l'identificazione del segnalante può essere condivisa, a meno che non siano stati precedentemente resi anonimi.

Durante l'indagine, il *Responsabile dei sistemi interni di segnalazione* esamina le circostanze attraverso l'analisi dei documenti e dei dati disponibili nonché, se ritenuto utile/opportuno, intervistando il Segnalante e tutte le altre persone ritenute utili per la risoluzione del caso.

Le indagini devono essere condotte in modo professionale, nel rispetto di tutte le normative applicabili a tutela dei diritti di difesa delle persone interessate.

Se la segnalazione è stata inviata tramite linea telefonica o altro sistema di messaggistica vocale, la relazione orale deve essere documentata da:

- previo consenso, una registrazione della conversazione su un dispositivo idoneo alla conservazione e all'ascolto; o
- una trascrizione completa e accurata della conversazione con la persona incaricata; quest'ultima opzione deve consentire al Segnalante di verificare, modificare e approvare la trascrizione della chiamata mediante la propria sottoscrizione.

Se il segnalante chiede un incontro con il *Responsabile dei sistemi interni di segnalazione*, l'incontro deve essere documentato:

- effettuando, previo consenso, una registrazione della conversazione su un dispositivo idoneo alla conservazione e all'ascolto; o
- attraverso un verbale accurato della riunione che consenta al Segnalante di verificare, rettificare e confermare mediante la propria sottoscrizione.

Durante l'indagine, tutta la documentazione deve essere conservata su un supporto durevole che consenta un facile accesso alle informazioni, nel rispetto dei requisiti sulla privacy dei dati e per il tempo necessario a completare l'indagine.

Il *Responsabile dei sistemi interni di segnalazione* inoltre:

- mantiene le interlocuzioni con il Segnalante, a cui può chiedere, se necessario, integrazioni;
- fornisce al Segnalante risposte formali e fondate, che devono essere il risultato di un'accurata valutazione dei fatti;
- fornisce riscontro alla segnalazione entro tre mesi dalla data dell'avviso del ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

In caso la segnalazione sia considerata come una reale violazione delle disposizioni previste, il "*Responsabile*", con il coinvolgimento del Responsabile di *Chief Audit Office* e di eventuali altre strutture che hanno supportato lo svolgimento dell'indagine, produce un report sulla violazione della norma.

Le violazioni di particolare gravità, aventi ad oggetto un comportamento illegittimo particolarmente importante, in ragione della condotta sottostante e/o della figura professionale interessata devono essere oggetto di immediata comunicazione all'Amministratore Delegato, al Consiglio di Amministrazione e al Collegio Sindacale che provvederanno ad esaminarli alla prima seduta utile.

A titolo non esaustivo e meramente esemplificativo sono di seguito indicati alcuni comportamenti illegittimi:

- violazioni che facciano presumere perdite o mancati ricavi;

- violazioni che siano passibili di sanzione amministrativa e/o penale da parte delle Autorità giudiziarie e di Vigilanza competenti;
- violazione delle norme contenute nel D.Lgs. 231/2007 e successive modifiche, con particolare riferimento agli obblighi di segnalazione di operazione sospette, agli obblighi di adeguata verifica della clientela, di registrazione delle operazioni e di conservazione.

Analogo procedimento viene applicato dal Responsabile di *Chief Audit Office* o da altri soggetti quando chiamati alla trattazione della segnalazione ai sensi del paragrafo 3.5.

### **3.8. DEFINIZIONE DELLE MISURE CORRETTIVE**

Il “*Responsabile dei sistemi interni di segnalazione*”:

- identifica, di concerto con ogni altra funzione competente ed in particolare con il Responsabile di *Chief Audit Office*, le eventuali misure correttive da attuare (interventi su processi, procedure o presidi di controllo) e le relative tempistiche;
- valuta l’opportunità di proporre sanzioni disciplinari, in conformità con la disciplina di legge e del contratto nazionale;
- invia le evidenze raccolte ai soggetti preposti ai provvedimenti decisionali, per la valutazione di eventuali provvedimenti disciplinari da adottare;
- nel caso di violazioni di particolare gravità, trasmette, previa comunicazione a *Chief Audit Office*, il Report all’Amministratore Delegato, al Consiglio di Amministrazione e al Collegio Sindacale e, per le violazioni rilevanti ai fini del D.Lgs. n. 231/2001 all’Organismo di Vigilanza;
- informa il segnalante dell’esito sintetico della Segnalazione e, in caso in cui non siano previste sanzioni disciplinari, anche il soggetto segnalato. Nel caso in cui siano previste sanzioni disciplinari è compito dei soggetti preposti ai provvedimenti decisionali informare il soggetto segnalato.

Nel caso in cui il Segnalante sia corresponsabile delle violazioni, deve essere applicato un trattamento privilegiato per quest’ultimo rispetto agli altri corresponsabili, compatibilmente con la disciplina applicabile. Di questo deve essere fornita adeguata informativa ai soggetti preposti ai provvedimenti decisionali.

### **3.9. PROVVEDIMENTI DECISIONALI**

La decisione sui provvedimenti da emettere nei confronti del personale coinvolto nelle violazioni compete:

- per i dipendenti della Capogruppo e/o delle altre società del Gruppo bancario, a *Chief People Office*, sentito l’organo con funzione di gestione (Amministratore Delegato, Consigliere Delegato), in qualità di struttura deputata ad eseguire i provvedimenti disciplinari del personale dipendente;
- per i Consulenti Finanziari, al Comitato Disciplinare previsto dalla specifica normativa interna;
- per i componenti degli Organi Sociali, al Consiglio di Amministrazione e/o al Collegio Sindacale a seconda dei casi, i quali, in base alle rispettive competenze, procederanno ad assumere le iniziative più opportune e adeguate coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto;
- per i soggetti terzi (fornitori, consulenti, etc) all’organo con funzione di gestione (Amministratore Delegato, Consigliere Delegato) che decide, caso per caso, l’adozione dell’azione da intraprendere (es: rescissione contratto fornitura/ consulenza, etc.).

### 3.10. MONITORAGGIO

Il Responsabile di Chief Compliance Office e il Responsabile di *Chief Audit Office* monitorano che le eventuali misure correttive identificate siano effettivamente messe in atto nei tempi concordati. A tal fine le eventuali strutture coinvolte nella realizzazione delle azioni correttive (es. *Chief People Office*) sono tenute ad informare, per competenza, il soggetto che ha gestito la segnalazione (Responsabile di Chief Compliance Office o Responsabile di Chief Audit Office) in merito all'evasione delle misure correttive. Qualora le misure correttive siano relative a violazioni in materia di antiriciclaggio e di prevenzione del finanziamento del terrorismo, il monitoraggio è condotto con la collaborazione del Responsabile di *Chief Anti Financial Crime Office*, che trasmette periodicamente un'informativa in merito al Responsabile di *Chief Compliance Office*.

Il Responsabile di *Chief Compliance Office* e il Responsabile di *Chief Audit Office* monitorano periodicamente l'evasione delle misure correttive identificate in relazione alle segnalazioni di rispettiva competenza.

### 3.11. MISURE DI PROTEZIONE E ANTI-RITORSIONE

Tutte le segnalazioni sono trattate e classificate con il livello massimo di riservatezza ed è garantita in ogni caso la riservatezza e la protezione dei dati personali del soggetto segnalante e del soggetto eventualmente segnalato<sup>1</sup>.

La Banca garantisce la riservatezza dell'identità del Segnalante, fatta eccezione per i casi in cui:

- il Segnalante esprima il proprio consenso alla comunicazione;
- la sua comunicazione sia richiesta dalla legge (ad esempio, quando le informazioni richieste sono necessarie per le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione);
- la sua conoscenza sia indispensabile per la difesa del soggetto segnalato.

I Segnalanti in buona fede sono garantiti e tutelati contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, a prescindere dai soggetti coinvolti.

Il Segnalante non subirà condotte ritorsive o discriminatorie o comunque sleali per aver effettuato la segnalazione. Qualsiasi forma di ritorsione, anche vessatoria, è vietata e pertanto sarà passibile di provvedimento disciplinare.

Le misure di protezione si applicano anche ai facilitatori ed altri soggetti in stretto legame (di tipo familiare e/o lavorativo) con il Segnalante secondo quanto previsto dal D.lgs. n. 24/23.

La protezione dalle ritorsioni è estesa anche al Segnalante che ha effettuato una segnalazione esterna alle autorità competenti quando il Segnalante:

- ha previamente effettuato una segnalazione interna e la stessa non ha avuto seguito;
- o ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- o ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

La protezione dalle ritorsioni è estesa anche al Segnalante che ha effettuato una divulgazione pubblica quanto il Segnalante:

---

<sup>1</sup> Gli obblighi di riservatezza non possono essere opposti quando le informazioni richieste sono necessarie per le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione.

- ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro entro i termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
- o ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa;
- o ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Resta inteso che le segnalazioni devono essere circostanziate e fondate su elementi di fatto precisi e concordanti.

Sono fonte di responsabilità, in sede disciplinare, eventuali forme di abuso della presente Policy, quali le segnalazioni effettuate al solo scopo di danneggiare il denunciato o altri soggetti, e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione del sistema di segnalazione.

La documentazione relativa alle segnalazioni è confidenziale. Tale documentazione deve essere archiviata in maniera sicura e nel rispetto delle norme vigenti all'interno della Banca sulla classificazione e trattamento delle informazioni ed in conformità alla normativa e regolamentazione locale<sup>2</sup>. Tale documentazione deve essere archiviata presso la struttura del "Responsabile" e presso la Funzione che ha effettuato la verifica e resa accessibile comunque solo ai dipendenti autorizzati.

### **3.12. OBBLIGHI INFORMATIVI E REPORTING**

Il *Responsabile dei sistemi interni di segnalazione* assicura la messa a disposizione di informazioni chiare sui sistemi interni di segnalazione, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale di segnalazione, sulle procedure e sui presupposti per effettuare le segnalazioni all' Autorità nazionale anticorruzione (ANAC)<sup>3</sup>.

A tal fine la presente Policy e le informazioni di cui sopra sono pubblicate sul sito [bancagenerali.com](http://bancagenerali.com) e sull'intranet aziendale.

Il *"Responsabile dei sistemi interni di segnalazione"* annualmente redige una relazione sul corretto funzionamento dei sistemi interni di segnalazione, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute.

La relazione è quindi messa a disposizione del Personale della Banca in un'apposita sezione della intranet aziendale.

---

<sup>2</sup> I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente. Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

<sup>3</sup> Ai sensi dell'art. 6 del d.lgs. 24/23

## 4. Gestione della policy e riferimenti normativi

### 4.1. GESTIONE DEL DOCUMENTO

La presente *Policy* è adottata con delibera di approvazione del Consiglio di Amministrazione della Banca.

Eventuali modifiche della *Policy*, necessarie e/o opportune classificate come “di minore rilevanza” ai sensi della *Policy di indirizzo per la redazione e aggiornamento di Policy e Regolamenti aziendali*, sono approvate dall’Amministratore Delegato su proposta dell’*Owner* (come *infra* definito) e da *Normativa e Regulatory Hub*, sentite eventualmente *Chief Compliance Office* e *Corporate Affairs*.

*Chief Compliance Office* (di seguito, l’“*Owner*”) è responsabile della verifica, con frequenza annuale dalla data di emanazione/ultima revisione, dell’eventuale necessità di aggiornamento della *Policy*, tenuto conto della rispondenza della stessa al contesto normativo di riferimento, alla strategia della Banca e dell’intero Gruppo e al contesto operativo e organizzativo in cui la Banca e il Gruppo operano.

### 4.2. RIFERIMENTI NORMATIVI

#### Normativa esterna

- Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Decreto Legislativo 10 marzo 2023, n. 24 “Attuazione della direttiva UE 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”;
- “Testo Unico Bancario”, D.Lgs. n. 385 del 1° settembre 1993 e successive modifiche ed integrazioni;
- “Testo Unico della Finanza”, D.Lgs. n. 58 del 24 febbraio 1998 e successive modifiche ed integrazioni;
- “Codice delle Assicurazioni Private”, D.Lgs. n. 209 del 7 settembre 2005 e successive modifiche ed integrazioni;
- D.Lgs. 21 novembre 2007 n. 231 e successive modifiche ed integrazioni;
- D.Lgs. 25 maggio 2017, n. 90 e successive modifiche ed integrazioni;
- Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, D.Lgs. 231 del 8 giugno 2001 e successive modifiche e integrazioni;
- “Codice in materia di Protezione dei Dati Personali”, D.Lgs. 196 del 30 giugno 2003 e successive modifiche e integrazioni;
- Circolare di Banca d’Italia “Disposizioni di vigilanza per le Banche” n. 285 del 17 dicembre 2013 e successive modifiche ed integrazioni;
- Codice di autodisciplina per le società quotate di Borsa Italiana.

### Normativa interna

- Codice Interno di Comportamento di Banca Generali;
- Documento illustrativo del Modello di Organizzazione e Gestione ex D.Lgs. n. 231/2001;
- Internal Fraud Policy di Banca Generali;
- CCNL credito;
- Regolamento disciplinare aziendale.

### **4.3. PERIMETRO DI APPLICAZIONE**

La presente *Policy* si applica a Banca Generali e alle Controllate del Gruppo bancario. Queste ultime recepiscono la *Policy* nel rispetto dei requisiti legali e regolamentari applicabili per attività o per luogo di costituzione. Nel caso in cui alcune delle previsioni contenute nella *Policy* dovessero essere meno restrittive rispetto alla normativa locale, la società interessata adotterà la norma locale vigente più restrittiva.

Gli organi con funzione di supervisione strategica delle Controllate del Gruppo bancario, tramite apposita delibera, sono tenuti a recepire la *Policy* adottata dalla Capogruppo, assumendo in tal modo la responsabilità di garantirne la conoscenza e assicurarne l'applicazione nell'ambito di rispettiva pertinenza e *business*, declinandola nella propria struttura organizzativa. Nel caso in cui emergano conflitti con normative o regolamenti locali, oppure in applicazione del principio di proporzionalità sorga l'esigenza di derogare dalla *Policy*, l'Organo con Funzione di Gestione (e.g., consigliere delegato/*general manager*) della società del Gruppo interessata fornisce preventivamente esplicita e motivata evidenza delle deroghe necessarie alla Capogruppo.

## 5. Glossario

### **Banca Generali o Banca o Società o Capogruppo**

Banca Generali S.p.A.

### **Cod. civ**

Il Codice civile

### **Codice di Corporate Governance**

Il Codice di *Corporate Governance* approvato dal Comitato per la *Corporate Governance* e promosso da Borsa Italiana S.p.A.

### **Controllate del Gruppo Bancario**

Le società bancarie, finanziarie e strumentali – con sede legale in Italia e all'estero – tempo per tempo controllate dalla Società e appartenenti al Gruppo Bancario

### **D.Lgs. n. 24/23**

Decreto Legislativo 10 marzo 2023, n. 24 “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”

### **Disposizioni di Vigilanza**

“*Disposizioni di vigilanza per le banche*” adottate con Circolare di Banca d’Italia n. 285 del 17 dicembre 2013

### **Divulgazione pubblica**

Una situazione in cui una persona rende di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone

### **Facilitatore**

Una persona che assiste una persona segnalante nel processo di segnalazione, operante all’interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata

### **Gruppo Bancario Banca Generali o Gruppo Bancario**

Il gruppo composto dalle società bancarie, finanziarie e strumentali – con sede legale in Italia e all’estero – tempo per tempo controllate dalla Società e facente capo a Banca Generali

### **Gruppo Generali**

Il gruppo societario facente capo ad Assicurazioni Generali S.p.A. e composto dalla stessa e dalle società da essa controllate ai sensi dell’art. 2359 commi 1 e 2 del Cod. civ.

**Gruppo Societario o Gruppo**

Il gruppo societario composto dall'insieme di società tra loro collegate in virtù di un rapporto di controllo da parte di Banca Generali

**Preoccupazione**

Conoscenza o ragionevole sospetto su una pratica o condotta considerata, in buona fede, inappropriata o incompatibile con la legge e/o la normativa interna.

**Responsabile dei sistemi interni di segnalazione o Responsabile**

Responsabile di *Chief Compliance Office*

**Ritorsione**

Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.

**Segnalanti o Beneficiari del sistema di segnalazione**

I soggetti come definiti al paragrafo 3.1 che prestano la loro attività lavorativa o intrattengono rapporti con la Banca o il Gruppo Bancario, che possono effettuare segnalazioni ai sensi della normativa vigente e della *Policy*

**TUB**

Il Decreto Legislativo 1° settembre 1993, n. 385, come successivamente modificato e integrato (Testo Unico delle leggi in materia bancaria e creditizia)

**Violazioni**

Comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità di Banca Generali che consistono negli illeciti, atti, comportamenti, condotte più specificamente indicati all'art. 2 del d.lgs. 24/23, comma 1