POLICY IN MATERIA DI SEGNALAZIONE INTERNA DELLE VIOLAZIONI – *WHISTLEBLOWING*

Approvata dal Consiglio di Amministrazione nella seduta del 23/05/2024.

Il presente documento abroga e sostituisce il precedente.

INDICE

1. PREMESSE E OBIETTIVI DEL DOCUMENTO

La tematica oggetto della presente policy è meglio nota con l'espressione anglosassone "whistleblowing". Si definisce **"**whistleblower" la persona che segnala comportamenti illeciti o violazioni di normative di cui è testimone all'interno dell'organizzazione o azienda, pubblica o privata, in cui lavora.
La traduzione più diffusa in italiano del termine "whistleblower" è "segnalante".

Riguardo al Whistleblowing, si evidenzia che la Banca ha, già da tempo, adottato un sistema interno di segnalazione, in ottemperanza alle normative speciali tempo per tempo vigenti ed applicabili alla Banca medesima, tra cui si ricordano la Circolare n. 285 del 17 dicembre 2013 e s.m.i., il TUB, il TUF, il CAP, la normativa sull'Antiriciclaggio e sul *Market Abuse*.

A seguito della introduzione nell'ordinamento nazionale del D.lgs. 10 marzo 2023, n. 24 ossia di una disciplina che tutela le persone che segnalano violazioni di "qualunque tipo" (di cui quelle relative al modello 231 sono un di cui), la Banca ha ritenuto opportuno abrogare e sostituire la previgente "Policy in materia di segnalazione interna delle violazioni – Whistleblowing", approvata dal Consiglio di Amministrazione nella seduta del 26/05/2021, con il presente documento, al fine di regolamentare la materia secondo quanto previsto dalla recente normativa richiamata e di estendere l'uso del suddetto canale alle altre ipotesi di violazione delle norme ivi citate.

Obiettivo prioritario della presente Policy è, dunque, quello di descrivere i presidi approntati dalla Banca allo scopo di consentire, ai Destinatari (come definiti al successivo paragrafo 3), la segnalazione di violazioni potenziali e/o effettive dei principi contenuti nel Modello 231, nonché delle disposizioni normative nazionali o dell'Unione europea (una cui completa illustrazione è contenuta nel successivo paragrafo 2) di cui siano venuti a conoscenza nello svolgimento della propria attività lavorativa.

Il processo stabilito è improntato al principio di proporzionalità, in relazione all'operatività e al contesto di riferimento della Banca.

Il sistema di Whistleblowing adottato dalla Banca individua in particolare:

- i soggetti abilitati ad effettuare le segnalazioni;
- l'oggetto e i contenuti della segnalazione;
- i soggetti responsabili dei sistemi interni di segnalazione delle violazioni e le funzioni aziendali coinvolte;
- i canali di comunicazione e le modalità che consentano un adeguato svolgimento delle procedure di *whistleblowing* permettendo un appropriato invio e una conseguente corretta ricezione, analisi e valutazione delle segnalazioni garantendo l'indipendenza valutativa e la completa trasparenza e tracciabilità dell'iter seguito;
- i procedimenti da attivare successivamente alla segnalazione;
- le forme di tutela che, con l'introduzione della normativa in materia di sistemi di segnalazione delle violazioni, devono essere riconosciute ai soggetti segnalanti, al fine di evitare possibili condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
- la tutela della riservatezza del contenuto della segnalazione e dell'identità del soggetto Segnalante e del Segnalato, nel rispetto della normativa applicabile anche in materia di protezione dei dati personali, fermi restando eventuali provvedimenti delle Autorità in relazione ai fatti oggetto

della segnalazione.
Sotto tale ultimo aspetto, in ottemperanza a quanto previsto dall'art. 13 del D.lgs. n. 24/2023, la Banca, in qualità di Titolare del trattamento, pone in essere gli adempimenti finalizzati a garantire la tutela dei dati personali trattati in caso di segnalazione ed in particolare si impegna a:

- garantire il principio di minimizzazione;
- definire il periodo e le modalità di conservazione dei dati personali;
- garantire il rispetto del principio di Privacy by Design & Default;
- garantire la riservatezza dell'identità del segnalante e del segnalato secondo le logiche descritte dall'art. 12 D. Lgs. 24/2023.

2. NORMATIVA DI RIFERIMENTO

Si riportano di seguito i principali riferimenti normativi che, in ambito bancario e finanziario, incidono in materia di whistleblowing:

- Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori);
- Legge 10 ottobre 1990, n. 287 (norme per la tutela della concorrenza e del mercato);
- Art. 52 – bis D. Lgs. 1° settembre 1993, n. 385 e s.m.i (T.U.B.);
- Art. 4 – *undecies* D. Lgs. 24 febbraio 1998, n. 58 e s.m.i. (T.U.F.);
- Art. 6 D. Lgs. 8 giugno 2001 n. 231 e s.m.i. così come modificato dall'art. 24 del D.Lgs. 10 marzo 2023, n. 24;
- Art. 10-quater D. Lgs. 7 settembre 2005, n. 209 e s.m.i.; (C.A.P.);
- Art. 48 D. Lgs. 21 novembre 2007, n. 231e s.m.i.;
- Circolare di Banca d'Italia n. 285 del 2013 e s.m.i. - Parte I, Titolo IV, Capitolo 3, Sezione VIII, "Sistemi interni di segnalazione delle violazioni";
- Regolamento (UE) n. 596/2014 (Regolamento sugli abusi di mercato);
- Regolamento (UE) n. 1286/2014;
- Regolamento Banca d'Italia di attuazione degli articoli 4-undecies e 6, comma 1, lettere b) e cbis), del TUF- Allegato 4 "Sistemi interni di segnalazione delle violazioni" così come modificato dal Provvedimento 23 dicembre 2022;
- Decreto Legislativo n. 196/2003 (Codice in materia di protezione dei dati personali, così come aggiornato dal Decreto Legislativo n. 101/2018);
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016(GDPR);
- Decreto Legislativo n. 24/2023 e relativo Allegato 1 (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).

3. DESTINATARI

Destinatari della presente Policy, in quanto soggetti abilitati, secondo normativa, ad effettuale le segnalazioni c.d. "Segnalanti**"** o "Segnalatori") sono:

a) i lavoratori subordinati, ivi compresi:

- i lavoratori il cui rapporto di lavoro è disciplinato dal d.lgs. n. 81/2015. Si tratta, ad esempio, di rapporti di lavoro a tempo parziale, intermittente, tempo determinato, somministrazione, apprendistato, lavoro accessorio;
- i lavoratori che svolgono prestazioni occasionali;

b) i lavoratori autonomi che svolgono la propria attività lavorativa presso la Banca;
c) i collaboratori a qualunque titolo che svolgono la propria attività lavorativa presso la Banca;
d) i liberi professionisti e i consulenti che prestano la propria attività presso la Banca;
e) i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la Banca;
f) gli azionisti della Banca e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, presso la Banca, anche qualora tali funzioni siano esercitate in via di mero fatto.

Ai Destinatari della presente policy è richiesto di segnalare eventuali comportamenti illeciti, anche solo tentati o che si abbia fondato motivo di ritenere che siano stati realizzati di cui siano venuti a conoscenza nell'ambito del proprio contesto lavorativo.
La tutela opera anche:
- se il rapporto giuridico non è iniziato (selezione e fasi precontrattuali);
- durante il periodo di prova;
- dopo lo scioglimento del rapporto (se le informazioni sono state acquisite in corso di rapporto).

I segnalanti beneficiano di misure di protezione a condizione che abbiano avuto fondati motivi di ritenere che le informazioni segnalate siano vere al momento della segnalazione e che tali informazioni rientrino nell'ambito di applicazione della disciplina.
Si precisa inoltre che le misure di protezione previste per il soggetto segnalante si applicano, ai sensi dell'art. 3, comma 5, lett. c del D.Lgs. 24/23 anche:
- ai cosiddetti facilitatori (coloro che prestano assistenza al lavoratore nel processo di segnalazione);
- alle persone del medesimo contesto lavorativo della persona segnalante e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado o colleghi che abbiano rapporti abituali e correnti di qualunque tipo;
- agli enti di proprietà della persona segnalante o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

Si rappresenta che, per effettuare la segnalazione non è necessario che il Segnalante disponga di prove della violazione, tuttavia, deve disporre di informazioni sufficientemente circostanziate che ne facciano ritenere ragionevole l'invio.

4. OGGETTO E CONTENUTI DELLA SEGNALAZIONE

4.1 Oggetto della segnalazione

Per "Segnalazione" si intende la comunicazione di possibili comportamenti illeciti, commissivi o omissivi che costituiscano o possano costituire una violazione o induzione a violazione di leggi e/o regolamenti rilevanti per il Whistleblowing indicate in precedenza, di valori e/o principi sanciti nel Codice Etico, nei principi di controllo interno, oltre che nelle policy e/o norme aziendali. Ai sensi dell'art. 52 bis, comma 1 del TUB, la segnalazione deve riguardare ogni atto o fatto che possa costituire una violazione delle norme disciplinanti l'attività bancaria - intendendo come tale quella

disciplinata dall'articolo 10 commi 1, 2 e 3 del TUB [1]- nonché ogni sospetto che si sia verificata o che si possa verificare ogni altra violazione relativa all'attività di raccolta del risparmio (ad esempio, la vendita di prodotti o servizi bancari), di esercizio del credito (ad esempio, la concessione di finanziamenti o crediti di firma), finanziaria (ad esempio, la prestazione di servizi di investimento) nonché ogni violazione relativa ad attività connesse o strumentali a quella bancaria. La segnalazione, anche se anonima, deve contenere una circostanziata descrizione dei fatti e dei comportamenti considerati in contrasto con la normativa indicando, ove possibile, anche i documenti, le regole che si considerano violate e gli altri riscontri utili a condurre l'accertamento sui fatti contestati. Inoltre, il segnalante ha l'obbligo di dichiarare se ha un interesse personale collegato alla segnalazione
Le segnalazioni hanno per oggetto:
1) illeciti amministrativi, contabili, civili o penali;
2) condotte illecite e rilevanti ai sensi del D.Lgs. 231/2001, o violazione dei modelli di organizzazione e gestione;
3) illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione Europea o nazionali indicati nell'allegato 1 al decreto legislativo n.24 del 2023 o degli atti nazionali che costituiscono attuazione degli atti dell'Unione Europea indicati nell'allegato alla Direttiva 2019/1937, seppur non indicati nell'allegato al suddetto decreto relativamente ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari; prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza degli alimenti, dei mangimi e della salute e benessere degli animali; sicurezza e conformità dei prodotti; sicurezza dei trasporti; salute pubblica; tutela della vita privata e protezione dei dati personali; tutela dell'ambiente; radioprotezione e sicurezza nucleare; protezione dei consumatori; sicurezza delle reti e dei sistemi informativi;
4) atti o omissioni che ledono gli interessi finanziari dell'unione europea (art 325 TFUE);
5) atti e omissioni riguardanti (art 26, par 2 TFUE) la libera circolazione delle merci, delle persone, dei servizi e dei capitali nel mercato interno, comprese violazioni delle norme dell'Unione Europea in materia di:
a. concorrenza;
b. aiuti di Stato;
c. imposte sulle società.
6) atti o comportamenti che vanificano oggetto e finalità delle disposizioni Ue di cui ai punti 3,4 e 5.

I comportamenti oggetto di segnalazione hanno le seguenti caratteristiche:
- possono qualificarsi come commissivi di una specifica violazione o anche come semplicemente omissivi rispetto alla violazione medesima;
- possono riguardare una richiesta di violazione o l'induzione a commettere una violazione;
- sono idonei a recare un danno o un pregiudizio economico, patrimoniale o anche solo reputazionale. Le condotte illecite segnalate devono riguardare situazioni di cui il soggetto sia venuto direttamente a conoscenza.

Si evidenzia che le segnalazioni Whistleblowing in materia di antiriciclaggio non sostituiscono in alcun modo l'iter di segnalazione delle operazioni sospette e non manlevano i soggetti interessati

[1] "*1. La raccolta di risparmio tra il pubblico e l'esercizio del credito costituiscono l'attività bancaria. Essa ha carattere d'impresa.*

2. L'esercizio dell'attività bancaria è riservato alle banche.

3. Le banche esercitano, oltre all'attività bancaria, ogni altra attività finanziaria, secondo la disciplina propria di ciascuna, nonché attività connesse o strumentali. Sono salve le riserve di attività previste dalla legge".

dalle possibili conseguenze dell'omessa segnalazione tramite il canale dedicato alla segnalazione delle operazioni sospette.

Ai fini della loro trattazione ed istruzione, le segnalazioni si distinguono in:

➢ Segnalazioni riferite a reati in materia di corruzione: comprendono non solo l'intera gamma dei delitti contro la pubblica amministrazione (ipotesi di corruzione per l'esercizio della funzione, corruzione per atto contrario ai doveri d'ufficio e corruzione in atti giudiziari), ma anche le situazioni in cui, nel corso dell'attività amministrativa, si riscontri l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati, nonché i fatti in cui – a prescindere dalla rilevanza penale – venga in evidenza un mal funzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite. Si fa riferimento a titolo meramente esemplificativo, ai casi di sprechi, c.d. nepotismo, demansionamenti, ripetuto mancato rispetto dei tempi procedimentali, assunzioni non trasparenti, irregolarità contabili, false dichiarazioni, violazione delle norme ambientali e di sicurezza sul lavoro.

➢ Segnalazioni di violazioni del Codice Etico: si considerano tali tutte le segnalazioni afferenti alla violazione dei principi del Codice Etico nel contenuto di tempo in tempo vigente.

➢ Segnalazioni di violazioni delle disposizioni contenenti nel MOG: tutte le segnalazioni aventi ad oggetto il mancato rispetto di norme previste nell'ambito del sistema normativo interno e del Modello Organizzativo della Società, nonché eventi idonei, almeno astrattamente, a cagionare una responsabilità amministrativa della Società ai sensi del D.lgs. 231/2001, ivi inclusa la potenziale commissione di qualsivoglia reato presupposto della responsabilità amministrativa degli enti.

➢ Segnalazioni in malafede: segnalazioni che dagli esiti della fase istruttoria si rilevino prive di fondamento sulla base di elementi oggettivi comprovanti la malafede del segnalante, fatta allo scopo di arrecare un danno ingiusto alla persona segnalata.

➢ Segnalazioni circostanziate: segnalazioni in cui la narrazione da parte dell'autore, di fatti, eventi o circostanze che costituiscono gli elementi fondanti dell'asserito illecito (ad esempio tipologia di illecito commesso, periodo di riferimento, valore, cause e finalità dell'illecito, aree e persone interessate o coinvolte, anomalia sul sistema interno di controllo etc.) è effettuata con un grado di dettaglio sufficiente a consentire, almeno astrattamente, di identificare elementi utili o decisivi ai fini della verifica della fondatezza della segnalazione stessa.

Le segnalazioni circostanziate si distinguono a loro volta in:

- Segnalazioni circostanziate verificabili: qualora, considerati i contenuti della segnalazione, sia possibile in concreto, sulla base degli strumenti di indagine a disposizione, compiere verifiche sulla veridicità della segnalazione.
- Segnalazioni circostanziate non verificabili: qualora, considerati i contenuti della segnalazione, non sia possibile, sulla base degli strumenti di indagine a disposizione, compiere verifiche sulla veridicità della segnalazione e pertanto procedere alla successiva fase di accertamento.
- Segnalazioni anonime: segnalazioni in cui le generalità del segnalante non sono esplicitate, né sono individuabili in maniera univoca. Alle segnalazioni anonime si applicano, per quanto compatibili, le disposizioni della presente Policy, purché siano adeguatamente circostanziate e rese con dovizia di particolari, ove cioè siano in grado di far emergere fatti e situazioni relazionandoli a contesti determinati.

4.2 Contenuto della segnalazione

Al fine di consentire ai soggetti e/o agli organi preposti di procedere alle opportune analisi e verifiche, il *whistleblower*, previa informativa sul trattamento dei dati personali, è tenuto a fornire i seguenti elementi volti a circoscrivere il più possibile l'ambito della segnalazione e a riscontrare la fondatezza dei fatti oggetto di segnalazione:

- generalità del soggetto che effettua la segnalazione, con indicazione della posizione o funzione svolta nell'ambito dell'azienda;
- descrizione chiara e completa degli atti o fatti oggetto della segnalazione;
- se conosciute, le generalità, la qualifica e/o il ruolo che permettano di identificare il/i soggetto/i che hanno posto in essere i fatti oggetto della segnalazione;
- le circostanze di luogo e di tempo in cui sono state commesse le violazioni oggetto di segnalazione;
- l'inoltro di eventuali documenti che possano ulteriormente circoscrivere e/o confermare i fatti segnalati;
- la dichiarazione al Responsabile dei sistemi interni di segnalazione delle violazioni riguardo un suo eventuale interesse privato collegato agli atti o ai fatti comunicati tramite la segnalazione;
- dichiarazione di eventuali corresponsabilità riguardo alla violazione segnalata;
- qualsiasi altra informazione utile al riscontro della fondatezza dei fatti segnalati.

4.3 Esclusione della tutela

Al segnalante non vengono garantite le tutele previste nella presente Policy qualora la Segnalazione riporti informazioni false, rese con dolo o colpa grave (c.d. Segnalazione in "mala fede"); tale comportamento potrà dare luogo anche ad un procedimento disciplinare o azioni legali nei suoi confronti.

Restano escluse dalle segnalazioni ammissibili quelle aventi ad oggetto:

- contestazioni, rivendicazioni o richieste di carattere personale, che attengono ai rapporti individuali di lavoro / figure gerarchicamente sovraordinate/colleghi, per le quali occorre fare riferimento al competente ufficio U.S. Risorse Umane.
- segnalazioni di violazioni già disciplinate da leggi speciali, già regolate mediante regolamenti UE o Direttive già trasposte;
- Segnalazioni in materia di sicurezza e difesa, appalti nel settore difesa e sicurezza nazionale.

4.4 Informativa privacy

Con riferimento all'obbligo di informare i segnalanti, i segnalati e le ulteriori persone coinvolte nella segnalazione, in qualità di soggetti interessati al trattamento, circa modalità e finalità del trattamento stesso, nonché tutti gli ulteriori elementi previsti ai sensi degli art. 13 e 14 del GDPR, la Banca si impegna a:

- predisporre e formalizzare informative privacy da rendere agli interessati, definendone le modalità di trasmissione più idonee secondo il canale utilizzato;
- richiedere il consenso del segnalante per rivelare la sua identità a persone diverse dai soggetti autorizzati a gestire la segnalazione;
- rivelare l'identità del segnalante nel contesto del procedimento disciplinare – quindi anche al segnalato - nel solo caso in cui detto procedimento si fondi esclusivamente sul contenuto della

segnalazione, al fine di garantire il diritto di difesa del segnalato e, comunque, previo espresso consenso del segnalante;

– rispettare i principi di cui all'art. 14 c. 2-4 D. Lgs. 24/2023 in caso di segnalazioni effettuate oralmente.

5. SOGGETTI PREPOSTI E FUNZIONI COINVOLTE

5.1 Responsabile dei sistemi interni di segnalazione delle violazioni

L'Organismo di Vigilanza ex D. Lgs. 231/01 è il responsabile del sistema interno di segnalazione: assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio agli Organi aziendali le informazioni oggetto di segnalazione, ove rilevanti (di seguito "Responsabile" o "Gestore" o "OdV").

La Funzione U.S. Compliance collabora con l'OdV nell'attività istruttoria del processo di segnalazione, secondo quanto meglio specificato *infra.*

Tale scelta è dettata dalla volontà della Banca di sfruttare le conoscenze pregresse della suddetta funzione in materia di processi aziendali e di competenze nelle attività di indagine.

Secondo quanto previsto dalla normativa vigente, la figura del Responsabile dei sistemi interni di segnalazione delle violazioni deve presentare le seguenti caratteristiche:

– non essere gerarchicamente e funzionalmente subordinato all'eventuale soggetto segnalato;
– non deve essere esso stesso il presunto responsabile della violazione;
– non deve avere un potenziale interesse correlato alla segnalazione tale da compromettere l'imparzialità e l'indipendenza di giudizio.

Sono individuati quali soggetti preposti ad essere informati tempestivamente da parte del Responsabile riguardo a violazioni di particolare gravità:

- il Presidente del Consiglio di Amministrazione;
- l'Amministratore delegato;
- il Responsabile U.S. Risorse Umane.

La Banca individua nella Funzione U.S. Revisione Interna il soggetto preposto a ricevere direttamente le segnalazioni, mediante un canale alternativo previsto all'interno dell'applicativo informatico, qualora il primo grado di segnalazione indirizzata al Responsabile non sia andato a buon fine a causa delle seguenti motivazioni:

– negligenza o eccessivo ritardo nella risposta da parte dell'organo Responsabile dei sistemi interni di segnalazione delle violazioni;
– il Responsabile a ricevere le segnalazioni è esso stesso direttamente o indirettamente implicato nei fatti oggetto della segnalazione;
– altri motivi legati al malfunzionamento della procedura prevista.

Ai sensi dell'art. 29 GDPR, i soggetti di cui al presente paragrafo sono autorizzati formalmente al trattamento dei dati personali, ricevendo specifiche e adeguate istruzioni. Ciascuno di essi sottoscrive un'apposita lettera di autorizzazione, impegnandosi, tra le altre cose, a garantire la riservatezza delle informazioni trattate e ad utilizzare queste ultime nei limiti di quanto necessario alla gestione delle segnalazioni. Agli stessi è erogata la formazione privacy nell'ambito del sistema di segnalazione.

Ai sensi dell'art. 26 GDPR, laddove siano condivise risorse per il ricevimento e la gestione delle segnalazioni tra più soggetti inquadrabili come titolari del trattamento, tra i quali la Banca, gli stessi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali.

6. CANALI DI SEGNALAZIONE

6.1 Il canale di segnalazione interno

La Banca, sentite le Organizzazioni sindacali, ex art. 4 del D.lgs. n.24 del 2023, ha attivato un proprio canale interno di segnalazione, affidandone la gestione all'OdV.

Il canale di segnalazione garantisce la riservatezza:
- della identità della persona segnalante;
- della persona coinvolta o menzionata nella segnalazione;
- del contenuto della segnalazione;
- dei documenti connessi alla segnalazione.

La Banca, nell'ambito della sua autonomia organizzativa e secondo le proprie reali esigenze ha previsto le seguenti 3 forme di segnalazione:

a) <u>tramite procedura informatica</u>

In particolare, la procedura informatica adottata dalla Banca è individuata nell'applicativo dell'Intranet aziendale "*Whistleblowing*"; è destinata ai soli dipendenti e collaboratori abilitati ad accedere all'intranet aziendale e consente la gestione delle attività legate all'intero processo di segnalazione, tra cui si elencano le seguenti:

- Gestione riservata delle informazioni.
- Tutela del soggetto segnalante.
- Informativa al soggetto segnalante e segnalato.
- Fase di istruttoria successiva alla segnalazione.
- Inoltro di allegati e documenti.

b) <u>orale, tramite incontro diretto (su richiesta)</u>

Segnatamente, su richiesta della persona segnalante, quest'ultima viene convocata dall'ODV per un colloquio confidenziale diretto e relativa verbalizzazione dello stesso previa informativa sul trattamento dei dati personali e consenso del segnalante; detto verbale può essere verificato, rettificato e confermato dal segnalante mediante propria sottoscrizione.

c) <u>scritta, tramite segnalazione cartacea in busta chiusa</u>

In tale ultimo caso, la segnalazione può avvenire mediante documento cartaceo trasmesso in busta chiusa con l'indicazione "Segnalazione di Whistleblowing - documento riservato", tramite posta ordinaria, presso gli Uffici Direttivi della Banca siti in Via E. Albanese, 94 (Palazzo Petyx), 90139 - Palermo da indirizzare al Responsabile dei sistemi interni di segnalazione o in alternativa nei soli casi in cui quest'ultimo sia identificato quale presunto responsabile della violazione o abbia un potenziale interesse correlato alla segnalazione, alla U.S. Revisione Interna.
La segnalazione viene ricevuta dall'OdV che la gestirà mantenendo il dovere di confidenzialità nei confronti del segnalante e la trasmetterà alla Funzione Compliance per le relative attività istruttorie.
La U.S. Compliance, presa in carico la segnalazione, analizza l'evidenza ricevuta, esaminando innanzitutto la sua ricevibilità formale, anche attraverso approfondimenti con il segnalante.

Qualora la segnalazione non sia considerata ricevibile (ad es. perché palesemente infondata e/o non circostanziata), la U.S. Compliance propone all'Odv l'archiviazione, mantenendone evidenza.

Qualora la segnalazione sia ritenuta fondata, la U.S. Compliance:

- svolge l'istruttoria avvalendosi della documentazione fornita dal soggetto segnalante, ovvero ascoltando l'autore della segnalazione;

- conduce indagini (in loco o a distanza, anche utilizzando la propria struttura) tese ad accertare la presunta violazione. In tale contesto, ricorre ad analisi documentali, interrogazioni nei sistemi informativi aziendali, interviste al presunto autore del reato/violazione per ulteriori notizie ed informazioni;

- completata l'indagine (in tempo utile al rispetto del termine massimo di tre mesi dalla ricezione dell'evidenza, fermo restando casi di urgenza derivanti dalla gravità della presunta violazione, o termine maggiore per motivate ragioni), inoltra gli esiti della stessa all'ODV per la necessaria informativa e gli eventuali provvedimenti.

L'OdV tiene informato l'Amministratore Delegato, nel rispetto della normativa esterna ed interna vigente, mantenendo comunque segreta l'identità del Segnalante, salvo casi di legge o autorizzazione alla disclosure del Segnalante stesso.

In esito al processo sopra descritto, i competenti Organi aziendali, sempre nel rispetto della normativa esterna ed interna vigente, possono:

- adottare provvedimenti disciplinari previsti dalla regolamentazione vigente nei confronti dei soggetti segnalati riconosciuti responsabili delle violazioni, con un trattamento più favorevole per l'eventuale segnalante corresponsabile delle stesse con il segnalato.
- nel caso di segnalazione palesemente infondata, adottare provvedimenti disciplinari previsti dalla regolamentazione vigente nei confronti dei soggetti segnalanti che abbiano agito con dolo o colpa grave;
- provvedere alle relative segnalazioni alle Autorità di Vigilanza e/o alle competenti Autorità giudiziarie sui fatti rilevati, fatte salvi gli obblighi di legge.

L'Identità del segnalante può essere rivelata al segnalato solo quando la conoscenza sia indispensabile per la difesa del segnalato stesso e previo consenso espresso del segnalante.

6.2 Il canale di segnalazione esterna

La persona segnalante può effettuare una segnalazione esterna se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

- il canale di segnalazione interna ovvero non è attivo o non è conforme a quanto previsto dall'art. 4 del D.Lgs 24/2023;
- la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- la persona segnalante 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;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

6.2.1 Il soggetto destinatario della segnalazione esterna

La segnalazione esterna deve essere inoltrata all'Autorità Nazionale Anticorruzione (ANAC), che attiva un canale di segnalazione che garantisce, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

6.2.2 Modalità di effettuazione della segnalazione esterna

La segnalazione esterna può essere effettuata in forma scritta tramite piattaforma informatica, oppure in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale, ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole.
La segnalazione inoltrata a soggetto diverso da ANAC deve comunque essere inviata all'autorità competente entro 7 giorni dal suo ricevimento.

7. IDENTITA' DEL SEGNALANTE

Con riferimento all'eventuale palesamento dell'identità del segnalante, la Banca ai sensi della disciplina dei sistemi interni di segnalazione delle violazioni, prevede anche la trattazione di segnalazioni effettuate con le modalità dell'anonimato.

Restano fermi gli obblighi di riservatezza da parte del personale addetto alla gestione delle segnalazioni, di cui si tratta nel prosieguo del presente documento, nonché la possibilità di rivelarne l'identità ad altri soggetti solo previo consenso del segnalante.

La Banca garantisce l'esercizio dei diritti agli interessati, nei limiti di quanto previsto dall'articolo 2-undecies del Codice Privacy. A tal riguardo, il Titolare dispone di una procedura di gestione delle richieste degli interessati, alla quale si rinvia. La possibilità di accogliere le richieste eventualmente pervenute viene bilanciata con il diritto alla riservatezza del segnalante e delle persone coinvolte.

8. OBBLIGHI DEL SEGNALANTE

Il soggetto segnalante è obbligato a dichiarare al Responsabile dei sistemi interni di segnalazione delle violazioni riguardo un suo eventuale interesse privato collegato agli atti o ai fatti comunicati tramite le segnalazioni.

9. OBBLIGHI DEL GESTORE DELLA SEGNALAZIONE

Il gestore della segnalazione deve:
- rilasciare alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
- fornire riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione;
- mantenere interlocuzioni con il segnalante;

- richiedere integrazioni al segnalante, se necessario;
- fornire "seguito" diligente alla segnalazione;
- mettere a disposizione informazioni chiare su canali, procedure e presupposti per effettuare segnalazioni interne ed esterne;
- esporre tali informazioni nei luoghi di lavoro o renderle accessibili per coloro che non li frequentano;
- pubblicare le informazioni in apposita sezione dedicata del sito web.

10. RISERVATEZZA E DIVIETO DI RITORSIONE

L'Organismo di Vigilanza - destinatario della segnalazione – e i soggetti coinvolti nell'attività istruttoria devono garantire la riservatezza del soggetto segnalante sin dal momento della presa in carico della segnalazione, anche nelle ipotesi in cui la stessa dovesse rivelarsi successivamente errata o infondata. Il venir meno di tale obbligo costituisce una violazione della procedura e, conseguentemente, del Modello 231. Il Segnalante, nell'ambito della propria attività di segnalazione, non subirà condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione medesima (a titolo di esempio: licenziamento, demansionamento, *mobbing,* ecc…) ed ha altresì il diritto, qualora sia ritenuto necessario, di chiedere il trasferimento in altro ufficio. La Banca si impegna a garantire, laddove ragionevolmente possibile, il soddisfacimento della predetta richiesta di trasferimento. La Banca si riserva il diritto di adottare le opportune azioni contro chiunque ponga in essere, o minacci di porre in essere, atti di ritorsione contro coloro che abbiano presentato Segnalazioni in conformità alla presente Policy, fatto salvo il diritto degli aventi causa di tutelarsi legalmente qualora siano state riscontrate in capo al Segnalante responsabilità di natura penale o civile legate alla falsità di quanto dichiarato o riportato.
Qualora il segnalante anonimo sia stato successivamente identificato e abbia subito ritorsioni, si applicano le misure di tutela e protezione testé descritte.

11. PROCEDURA INFORMATICA

Il processo di segnalazione è gestito anche mediante la specifica procedura informatica, denominata "Whistleblowing" sopra indicata disponibile nella intranet aziendale, che archivia i dati in forma protetta. La procedura consente di inserire la segnalazione, previa messa a disposizione dell'informativa privacy e raccolta di consenso per la rivelazione dell'identità del segnalante, garantendo sempre l'assoluta riservatezza dei dati del Segnalante, la confidenzialità delle informazioni fornite dallo stesso. Una volta inoltrata la Segnalazione tramite la procedura messa a disposizione, il Segnalante ha la possibilità di verificare in qualsiasi momento, accedendo nuovamente alla procedura, la conferma di ricezione della segnalazione, lo stato di avanzamento della pratica, e le eventuali richieste di approfondimenti e/o di ulteriore documentazione a supporto. L'Archivio delle segnalazioni garantisce la tracciabilità e l'archiviazione dei dati, garantendo la riservatezza o l'anonimato dei dati contenuti nelle singole pratiche.
Ove la Banca dovesse avvalersi di un fornitore esterno per la gestione delle segnalazioni (es. fornitori di piattaforme di whistleblowing), ai sensi dell'art. 28 GDPR, provvederà alla nomina per iscritto a responsabile del trattamento.

12. GESTIONE DELLA SEGNALAZIONE

Il compito di gestire le segnalazioni è affidato all' OdV, il quale si impegna a garantire:

- la conservazione della documentazione inerente alle Segnalazioni e le relative attività di verifica nonché gli eventuali provvedimenti decisionali adottati dalle funzioni competenti in appositi archivi cartacei/informatici, assicurando adeguati livelli di sicurezza/riservatezza;

- la conservazione della documentazione e delle Segnalazioni per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati e comunque nel rispetto della vigente normativa in tema di protezione dei dati personali.

Nei casi in cui il soggetto Responsabile del sistema interno di segnalazione, sia individuato come l'autore della presunta violazione o lo stesso abbia un potenziale interesse correlato alla segnalazione, la Segnalazione stessa dovrà essere passata alla competenza della Funzione U.S. Revisione Interna, che opererà ai sensi della presente Policy quale gestore delle segnalazioni alternativo (in luogo dell'OdV).

L'OdV potrà avvalersi del supporto oltre che della U.S. Compliance per lo svolgimento delle attività istruttorie, altresì di altre funzioni della Società o di consulenti specializzati, in base alle specifiche competenze richieste in relazione al contenuto della Segnalazione oggetto di verifica. Qualora, all'esito dell'attività di verifica, la segnalazione risulti fondata, l'OdV, in relazione alla natura della violazione accertata – oltre a condividere gli esiti con le funzioni e organi competenti – potrà presentare denuncia all'Autorità Giudiziaria.

13. COMPITI DELL'ODV

L'Organismo di Vigilanza ha piena visibilità delle segnalazioni e può decidere, con il supporto della U.S. Compliance, se avviare un processo di accertamento o archiviare la stessa, documentando, nell'ambito del verbale della riunione in cui la segnalazione è trattata, le motivazioni.

L'OdV provvede in particolare a:

- effettuare specifiche attività di accertamento con l'ausilio della U.S. Compliance e/o avvalendosi eventualmente di altre strutture aziendali in base alle specifiche competenze, oppure di consulenti esterni, ove necessario;
- interrompere le attività di approfondimento qualora, a seguito delle stesse, emerga l'infondatezza della Segnalazione.

L'OdV si impegna a fornire un primo riscontro al Segnalante entro 7 (sette) giorni dal ricevimento della Segnalazione. L'OdV si adopera affinché le Segnalazioni vengano processate entro un tempo ragionevole. La durata del processo istruttorio non può superare di norma i tre mesi, fatte salve circostanze particolari da provare e documentare. Durante la fase di istruttoria l'OdV e/o la U.S. Compliance potranno informare il Segnalante circa lo stato della propria Segnalazione, anche ponendo a quest'ultimo eventuali ulteriori domande e richieste di chiarimento in merito alla Segnalazione.

Nella fase di istruttoria e verifica l'OdV e la Funzione U.S. Compliance:

- garantiscono l'imparzialità, l'equità e l'accuratezza dell'analisi e valutazione della segnalazione;
- assicurano la confidenzialità delle informazioni raccolte e della riservatezza dell'identità del Segnalante.

Al termine delle attività di accertamento/approfondimento, e sulla base degli esiti della stessa, l'Organismo di Vigilanza:

a. archivia il caso laddove la segnalazione risulti infondata;
b. richiede ulteriori approfondimenti;
c. comunica alle funzioni interessate le raccomandazioni del caso;
d. valuta con strutture aziendali competenti eventuali provvedimenti disciplinari da irrogare nei riguardi dei soggetti coinvolti ed eventuali azioni a tutela degli interessi dell'azienda, nel rispetto della normativa vigente.
Una volta chiusa l'istruttoria il segnalante verrà informato dell'esito.

14. SISTEMA SANZIONATORIO

All'esito delle attività di istruttoria e verifica, l'OdV, qualora la segnalazione sia stata ritenuta fondata, inoltra le informazioni ricevute all'Amministratore delegato, che con l'ausilio della U.S. Risorse Umane provvederà ad attivare le dovute azioni disciplinari e/o ad irrogare le eventuali sanzioni a carico dei soggetti responsabili qualora sia stato appurato che i fatti contenuti nella segnalazione abbiano violato o arrecato pregiudizio a norme disciplinanti l'attività svolta all'interno della propria funzione di competenza.
Sono fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente Policy, quali le Segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il denunciato o altri soggetti e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente Policy.
Nel caso in cui il Segnalante sia corresponsabile delle violazioni, è previsto un trattamento privilegiato per quest'ultimo rispetto agli altri corresponsabili, compatibilmente con la violazione commessa e con la disciplina applicabile.

15. GARANZIE INERENTI AL SISTEMA DI SEGNALAZIONE (WHISTLEBLOWING)

La violazione degli obblighi di riservatezza dei dati del Segnalante è ritenuta alla stregua di una violazione del Modello 231 e sarà sanzionata ai sensi del Sistema sanzionatorio e disciplinare di cui al Modello 231. La Banca non tollera minacce, ritorsioni e/o discriminazioni nei confronti di colui che, in buona fede, segnala condotte illecite e/o non conformi al D.Lgs. n. 231/2001 o ad altre normative in vigore.
Per quanto riguarda la posizione di chi effettua una segnalazione, la norma prevede:
- il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati direttamente o indirettamente alla segnalazione;
- sanzioni nei confronti di chi viola le misure poste a tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelino infondate;
- la nullità del licenziamento ritorsivo o discriminatorio del segnalante;
- la denuncia all'Ispettorato Nazionale del Lavoro di misure discriminatorie nei confronti del segnalante.

I Canali di segnalazione interna adottati dalla Banca assicurano, anche tramite l'eventuale ricorso a strumenti di crittografia, la riservatezza dell'identità del segnalante, del segnalato e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione, anche al fine di proteggere i soggetti indicati da possibili ritorsioni o discriminazioni.
Le generalità del segnalante non possono essere rivelate a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati dalla Banca, ai sensi della presente Policy. I suddetti dati possono essere diffusi all'esterno e comunicati a terzi nei soli casi previsti dall'art. 12 del D.lgs. n. 24 del 2023.

Resta ferma la protezione di informazioni classificate, coperte da segreto professionale forense e medico e degli organi giudiziari. Restano salve le applicazioni di norme procedura penale su segreto (articolo 329 cpp).
Con riferimento a potenziali violazioni di dati personali (Data Breach), si rinvia alla Policy di gestione dei Data Breach in essere presso la Banca.

16. RESPONSABILITÀ DEL WHISTLEBLOWER

La presente procedura lascia impregiudicata la responsabilità penale e disciplinare del segnalante nell'ipotesi di segnalazione calunniosa o diffamatoria ai sensi del Codice penale e dell'art. 2043 del codice civile.

17. FORMAZIONE

La presente Policy deve essere oggetto di ampia comunicazione, così da diventare un costante riferimento nelle attività aziendali. La Banca ha il dovere di attuare iniziative di comunicazione interna e di formazione agli Esponenti Aziendali ed al Personale sul funzionamento del Sistema di Whistleblowing adottato, indicando i presidi posti a garanzia della riservatezza dei dati personali (sia del Segnalante che del Segnalato), gli strumenti e le procedure da seguire per la gestione della segnalazione in tutte le sue fasi, dall'inserimento fino alla conclusione.
Per i collaboratori è prevista analoga informativa e pubblicità della procedura, anche secondo modalità differenziate, ad esempio attraverso consegna cartacea con ricevuta di presa visione.

18. REGISTRO

L'OdV redige ed aggiorna un registro delle eventuali Segnalazioni ricevute, annotandone gli elementi principali delle stesse.

19. REPORTING

L'OdV rende conto annualmente del corretto funzionamento dei sistemi interni di segnalazione, riportando nella propria relazione le informazioni aggregate sulle risultanze dell'attività svolta e sul seguito dato alle Segnalazioni ricevute; nella redazione di tale rendiconto, l'OdV è tenuto a rispettare quanto previsto dalla disciplina sulla protezione dei dati personali.

20. ARCHIVIAZIONE

Al fine di consentire la ricostruzione delle diverse fasi del processo assicurandone la tracciabilità, tutta la documentazione raccolta viene archiviata a cura del Responsabile dei Sistemi interni si segnalazione, su supporto informatico garantendo la riservatezza della documentazione acquisita attraverso un sistema di protezione dei dati, e deve essere accessibile esclusivamente al Responsabile dei sistemi di segnalazione interna e ai soggetti espressamente autorizzati dalla Banca in virtù del proprio ruolo. Detta documentazione viene conservata per un periodo non superiore a cinque anni dalla data di comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'art.12 del D.Lgs. 10 marzo 2023 n. 24 e della normativa europea e nazionale in materia di privacy.

21. ULTERIORI ADEMPIMENTI SULLA PROTEZIONE DEI DATI PERSONALI

La Banca si impegna inoltre a:

- effettuare un'analisi dei rischi, finalizzata a identificare e gestire i rischi secondo un approccio basato sulla loro probabilità ed impatto;

- condurre una DPIA finalizzata, tra l'altro, ad individuare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati;
- aggiornare il registro dei trattamenti;
- mappare i trasferimenti verso paesi terzi e le relative garanzie a supporto;
- definire e applicare procedure per la concessione, la modifica e la revoca dell'accesso al sistema whistleblowing;
- predisporre misure di sicurezza adeguate alla piattaforma di segnalazione;
- definire le modalità per la manutenzione del sistema di segnalazione.

22. ADOZIONE E REVISIONE DELLA POLICY

La presente Policy viene approvata dal Consiglio di Amministrazione della Banca ed è soggetta a monitoraggio periodico e revisionata, ogni qualvolta se ne ravvisi la necessità.
La Banca si assicura altresì che la presente Policy sia portata a conoscenza dei destinatari in maniera chiara, precisa e completa, e che vengano chiariti gli aspetti relativi ai diritti, ai doveri e alle tutele di ciascun soggetto interessato, sia esso il segnalante che il segnalato, a seconda che la segnalazione sia avvenuta nell'ambito del perimetro definito dal TUB o abbia ad oggetto altra fattispecie.
La funzione Compliance è tenuta a valutare la conformità della presente Policy alle disposizioni vigenti e provvede a verificare l'adeguatezza delle procedure.