POLICY SUL SISTEMA INTERNO DI SEGNALAZIONE DELLE VIOLAZIONI DEL GRUPPO BANCARIO IFIGEST (WHISTLEBLOWING)

Area	**Processi di Governo (GOV)**
Macro Ambito	
Ambito	**Definizione e Policy aziendali**
Perimetro di applicabilità	**Gruppo Bancario Ifigest**
Data creazione	
Tipologia di documento	**Policy**
Data approvazione CdA Banca Ifigest	
Data approvazione CdA Soprarno Sgr	
Data approvazione CdA Sevian	

INDICE

1. Premessa 1
2. Definizioni....0
3. Fonti Normative 1
4. segnalazione delle violazioni 2
   4.1 Ambito di applicazione 2
   4.2 Destinatari 3
   4.3 Tutela del Segnalante 4
   4.4 Nominatività delle Segnalazioni 6
   4.5 Responsabilità del segnalante 7
   4.6 Canale di Segnalazione Esterna (ANAC) 7
   4.7 Divulgazione pubblica....8
   4.8 Misure e provvedimenti sanzionatori di competenza dell'ANAC....8
5. Ruoli e Responsabilità 8
   5.1 Organi aziendali 8
   5.2 Responsabile del sistema delle segnalazioni delle violazioni 9
   5.3 Altre Funzioni e Direzioni coinvolte....9
   5.4 Controllo sul sistema di segnalazione delle violazioni 10
   5.5 Rapporti con l'Organismo di Vigilanza....10
   5.6 Trattamento dei dati personali nelle segnalazioni whistleblowing....11
6. Processo di gestione delle segnalazioni di violazione 12
   6.1 Canale e modalità di trasmissione delle segnalazioni 12
   6.2 Ricezione della segnalazione 13
   6.3 Segnalazioni "Telefoniche e orali" 13
   6.4 Esame della segnalazione 13
   6.5 Gestione delle segnalazioni rilevanti....14
   6.6 Valutazione della segnalazione 15
   6.7 Azioni 15
   6.8 Reporting 15
   6.9 Archiviazione, conservazione e tracciabilità delle segnalazioni 16
   6.10 Formazione 16
   6.11 Valutazione del sistema interno di segnalazione delle violazioni 16
7. Misure e provvedimenti sanzionatori 17

1. Premessa

Il Decreto Legislativo 10 marzo 2023, n. 24 ha recepito la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali [1]. Il decreto è entrato in vigore il 30 marzo 2023, ma le disposizioni in esso contenute hanno efficacia dal 15 luglio 2023.

La nuova normativa intende, da un lato, garantire la manifestazione della libertà di espressione e informazione, che comprende il diritto di ricevere o di comunicare informazioni, dall'altro, è uno strumento per contrastare (e prevenire) la corruzione, la cattiva amministrazione e la prevenzione di violazioni di legge nel settore pubblico e privato.

Scopo della presente Policy è quello di definire il sistema adottato dalle Banche/Società del Gruppo Bancario Ifigest (di seguito il "Gruppo"), in coerenza con le disposizioni tempo per tempo vigenti, in tema di sistemi interni di segnalazione delle violazioni, per favorire la presentazione di segnalazioni che possono portare all'emersione di comportamenti illegittimi e violazioni di norme e regolamenti da parte del Personale.

In particolare, il documento definisce criteri e modalità per la ricezione, l'analisi e il trattamento delle segnalazioni di violazioni, assicurando un'adeguata riservatezza e protezione dei dati personali del soggetto che effettua la segnalazione e del soggetto segnalato. Sono, inoltre, stabilite le precauzioni adottate a tutela del segnalante, quali la tutela dell'anonimato e il contrasto a ogni possibile discriminazione o ritorsione nei suoi riguardi, rimuovendo così i possibili fattori che potrebbero impedire o rendere difficoltosa la denuncia di illeciti comportamenti. Gli illeciti oggetto di segnalazione ai sensi della presente Policy sono indicati nel successivo par. 4.1.

2. Definizioni

Attività bancaria	Ai sensi dell'art. 10 del TUB: La raccolta di risparmio tra il pubblico e l'esercizio del credito nonché ad ogni altra attività finanziaria, secondo la disciplina propria di ciascuna e altre attività connesse o strumentali.
Canale	Mezzo fisico di comunicazione della segnalazione
Codice Etico	Codice Etico adottato dal Gruppo Bancario Ifigest
Modello 231	Il modello di organizzazione, gestione e controllo adottato dalla Banca ai sensi del D.Lgs. 8 giugno 2001, n. 231
O.d.V.	L'Organismo di Vigilanza nominato dal Consiglio di Amministrazione ai sensi del D.Lgs. 8 giugno 2001, n. 231 e s.m.i.
Organi Aziendali	Consiglio di Amministrazione, Collegio Sindacale, Amministratore Delegato/ Direttore Generale
Personale	a) Violazioni riconducibili all'Attività Bancaria, AML, TUF: dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato. b) Violazioni riconducibili al D.Lgs. n. 24/2023: dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma

[1] Il decreto è stato pubblicato nella Gazzetta Ufficiale, Serie generale n. 63 del 15 marzo 2023.

	diversa dal rapporto di lavoro subordinato ex art. 3, comma 3, dalla lett. c) alla lett. h) del D.lgs. n. 24/2023".
Responsabile	Il Responsabile del Sistema Interno di Segnalazione delle Violazioni della Banca/Società del Gruppo.
Segnalazione	• *Segnalazione interna*: qualsiasi comunicazione, nominativa ricevuta dalla Banca/Società del Gruppo effettuata da un soggetto riconosciuto quale appartenente al Personale della Banca/Società del Gruppo avente a oggetto fatti o comportamenti (di qualsivoglia natura, anche meramente omissivi) riferibili al Personale posti in essere in violazione di leggi o regolamenti o provvedimenti disciplinanti l'attività bancaria idonei ad arrecare danno o pregiudizio, anche solo d'immagine. • *Segnalazioni ex D.lgs. n. 24/2023*: o Segnalazione interna scritta: la comunicazione, effettuata in forma scritta, delle informazioni sulle violazioni, presentata tramite un canale di segnalazione interna. o Segnalazione interna orale: segnalazioni interne effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta del segnalante, mediante un incontro diretto fissato entro un termine ragionevole. o Segnalazione esterna: la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite un canale di segnalazione esterna attivato dall'ANAC.
Segnalazione diffamatoria o in "mala fede"	Segnalazione che, al termine della fase istruttoria, si rileva infondata ed effettuata in malafede, comunque, al solo fine di diffamare o cagionare un qualsiasi danno alla persona o alla società offesa
SISV o Sistema	Il Sistema Interno di Segnalazione delle Violazioni della Banca/Società del Gruppo.
ANAC	Autorità Nazionale Anticorruzione
Divulgazione pubblica o divulgare pubblicamente	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.

3. Fonti Normative

A seguire vengono riportate le principali fonti normative di riferimento della materia.

Direttiva 2013/36/UE del 26 giugno 2013 (Capital Requirement Directive – CRD IV)	Articolo 71 "Segnalazione delle violazioni"
Testo Unico Bancario	Decreto legislativo 1° settembre 1993, n. 385 – Art. 52 bis "Sistemi interni di segnalazione delle violazioni"
Testo Unico della Finanza	Decreto legislativo del 24 febbraio 1998, n. 58 - Art. 4-undecies "Sistemi interni di segnalazione delle violazioni", introdotto dal decreto 129/2017
Banca d'Italia	Circolare n. 285 del 17 dicembre 2013- SISTEMI INTERNI DI SEGNALAZIONE DELLE VIOLAZIONI (Parte I – Recepimento in Italia della CRD IV | Titolo IV – Governo societario, controlli interni, gestione dei rischi | Capitolo 3 – Il sistema dei controlli interni | Sezione VIII) e Sistemi interni di segnalazione delle violazioni – Resoconto della consultazione
Provvedimento della Banca D'Italia	Regolamento di attuazione degli articoli 4-undecies e 6, comma 1, lettere b) e c-bis), del TUF.

Normativa in materia di protezione dei dati personali	Regolamento (UE) 2016/679; D.lgs. n. 196/2003 e successive modifiche e integrazioni
GDPR	REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, del 27 aprile 2016, 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.
Legge n. 179/2017	Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato
D.Lgs. n. 231/2001 e s.m.i.	Responsabilità amministrativa delle società e degli enti
D.Lgs. n. 90/2017 e D. Lgs. n. 125/2019	Attuazione della direttiva UE 2015/849 (c.d. Quarta Direttiva Antiriciclaggio) relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonché' attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE.
D. Lgs. N. 24/2023	Decreto Legislativo 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
Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019	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.

4. segnalazione delle violazioni

4.1 Ambito di applicazione

Il *SISV d*elle *Banche/Società del Gruppo* fornisce al personale, così come definito nel Capitolo 2 della presente Policy, la possibilità di segnalare:

a) comportamenti, atti od omissioni che possano costituire una violazione delle norme disciplinanti l'*Attività bancaria*, ivi comprese violazioni potenziali o effettive delle disposizioni di prevenzione del riciclaggio e del finanziamento del terrorismo e di norme relative ai servizi di investimento e agli abusi di mercato nonché alle norme relative alla distribuzione dei prodotti assicurativi.
b) comportamenti, atti od omissioni che consistono in[2]:
   1) illeciti amministrativi, contabili, civili o penali;
   2) condotte illecite rilevanti del D. Lgs. n. 231/2001 o violazioni del MOG;
   3) illeciti rientranti nell'ambito degli atti dell'Unione europea o nazionale [3];
   4) atti od omissioni che ledono gli interessi finanziari dell'Unione;
   5) atti od omissioni riguardanti il mercato interno;
   6) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei punti 3, 4 e 5.

La Segnalazione è ammessa in tutte quelle circostanze in cui il segnalante, al momento della *Segnalazione stessa*, abbia una ragionevole certezza della correttezza delle informazioni fornite. I meccanismi a tutela del segnalante non

[2] Cfr. art. 2, comma 1, lett. a, punto 1, nn. da 1 a 6, D. Lgs. n. 24/2023.

[3] In particolare, per illeciti rientranti nell'ambito degli atti della normativa UE o nazionale, si intendono:

- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi.

sono, pertanto, da intendersi applicabili qualora siano fornite informazioni che il segnalante sappia essere errate, inaccurate o fuorvianti (c.d. "malafede").

La Segnalazione non può consistere in rivendicazioni, contestazioni, richieste di carattere personale della persona segnalante o della persona che abbia sporto una denuncia all'autorità giudiziaria o contabile, relative esclusivamente ai propri rapporti individuali di lavoro. Pertanto, i motivi che hanno indotto la persona a segnalare, denunciare o divulgare pubblicamente sono irrilevanti ai fini della trattazione della segnalazione e della protezione da misure ritorsive.

Le Segnalazioni devono essere circostanziate, qualificate e idonee a permettere di prevenire e/o reprimere comportamenti illeciti. È necessario, quindi, che la segnalazione sia il più possibile circostanziata al fine di consentire la delibazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni. In particolare, è necessario risultino chiare:

- le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- la descrizione del fatto;
- le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

È utile anche allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

4.2 Destinatari

La presente Policy si rivolge a tutto il Personale della Banca, come di seguito meglio indicato. La categoria qui definita dei "Destinatari" è riferibile al novero dei soggetti "segnalanti".

Con riferimento alle violazioni riconducibili all'attività Bancaria, AML e TUF, si intendono ricompresi nella definizione di Personale "i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato" ([4]).

Ai sensi del D.lgs. n. 24/2023, sono da intendersi come "Destinatari" nel settore privato le categorie di soggetti di seguito indicati:

- i lavoratori subordinati di soggetti del settore privato, ivi compresi i lavoratori il cui rapporto di lavoro è disciplinato dal decreto legislativo 15 giugno 2015, n. 81, o dall'articolo 54-bis del decreto-legge 24 aprile 2017, n. 50, convertito, con modificazioni, dalla legge 21 giugno 2017, n. 96;
- i lavoratori autonomi, ivi compresi quelli indicati al capo I della legge 22 maggio 2017, n. 81, nonché i titolari di un rapporto di collaborazione di cui all'articolo 409 del codice di procedura civile e all'articolo 2 del decreto legislativo n. 81 del 2015, che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato;
- i lavoratori o i collaboratori che svolgono la propria attività lavorativa presso soggetti del settore privato che forniscono beni o servizi o che realizzano opere in favore di terzi;
- i liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore privato;
- i tirocinanti che prestano la propria attività presso soggetti del settore privato;
- gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore privato.

La tutela delle persone segnalanti si applica, ai sensi del D.lgs. n. 24/2023 anche qualora la segnalazione, la denuncia all'autorità giudiziaria o contabile o la divulgazione pubblica di informazioni avvenga nei seguenti casi:

[4] Si tratta dei soggetti indicati nel successivo elenco, ad esclusione degli azionisti.

a) 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;

b) durante il periodo di prova;

c) successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

4.3 Tutela del Segnalante

La *Banca/Società del Gruppo* assicurano la riservatezza e la protezione dei dati personali del segnalante al fine di mitigare il rischio di ritorsioni e/o discriminazioni a suo carico; la documentazione relativa alle *Segnalazioni* è strettamente confidenziale.

Tutti i soggetti coinvolti nel processo hanno l'obbligo di garantire la confidenzialità delle informazioni ricevute e, in particolare, dell'identità del segnalante. La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatta salva ogni ulteriore forma di responsabilità prevista dalla legge.

L'identità del segnalante viene protetta a eccezione dei casi in cui:

- la S*egnalazione* risulti fatta allo scopo di danneggiare o altrimenti arrecare pregiudizio al segnalato (c.d. segnalazione in "malafede") e si configuri una responsabilità a titolo di calunnia o di diffamazione ai sensi di legge;
- l'anonimato non sia opponibile per legge (es. indagini penali, ispezioni di organi di controllo, indispensabili esigenze di difesa);
- nella *Segnalazione* vengano rivelati fatti e/o circostanze tali che, seppur estranei alla sfera aziendale, rendano opportuna e/o dovuta la segnalazione all'Autorità Giudiziaria.

I segnalanti non possono essere sanzionati, licenziati o sottoposti ad alcuna misura discriminatoria per motivi collegati, direttamente o indirettamente, alla segnalazione, salvo quanto precisato al Punto 4.5 e al Punto 7.

Per misure discriminatorie si intendono le azioni disciplinari ingiustificate, le molestie sul luogo di lavoro[5] e ogni altra forma di ritorsione [6].

Il D.Lgs. n. 24/2023[7] prevede, a tutela del segnalante, il divieto di ritorsione definita come "*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*"[8].

[5] Così come indicate nell'art. 17, comma 4, lett. g), D.Lgs. n. 24/2023 nel novero delle ritorsioni.

[6] L'art. 17, comma 4, D.lgs. n. 24/2023 contempla talune fattispecie di ritorsioni: a) il licenziamento, la sospensione o misure equivalenti; b) la retrocessione di grado o la mancata promozione; c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro; d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa; e) le note di merito negative o le referenze negative; f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria; g) la coercizione, l'intimidazione, le molestie o l'ostracismo; h) la discriminazione o comunque il trattamento sfavorevole; i) la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione; l) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; m) i danni, anche alla reputazione della persona, in particolare sui social media o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi; n) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro; o) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; p) l'annullamento di una licenza o di un permesso; q) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

[7] Cfr. art. 2, comma 1, lett. m, D.Lgs. n. 24/2023.

[8] Si tratta quindi di una definizione ampia del concetto di ritorsione che può consistere sia in atti o provvedimenti ma anche in comportamenti od omissioni che si verificano nel contesto lavorativo e che arrecano pregiudizio ai soggetti tutelati.
La nuova disciplina, fa riferimento unicamente alle ritorsioni, superando la suddivisione tra misure discriminatorie e ritorsioni presente nella L. n. 179/2017, e amplia notevolmente l'elencazione delle fattispecie che costituiscono ritorsioni, pur avendo questa un carattere

Si ribadisce che, affinché si possa configurare una ritorsione e, di conseguenza, il soggetto possa beneficiare di protezione è necessario uno stretto collegamento tra la segnalazione, la divulgazione e la denuncia e il comportamento/atto/omissione sfavorevole subito, direttamente o indirettamente, dalla persona segnalante, denunciante o che effettua la divulgazione pubblica.

Il segnalante che ritenga di aver subito una ritorsione deve darne notizia circostanziata al Presidente del Collegio Sindacale allo scopo di metterlo in grado di valutarne la fondatezza e adottare i possibili opportuni interventi.

I soggetti tutelati possono comunicare ad ANAC le ritorsioni che ritengono di aver subito, sia se trattasi di ritorsioni già compiute nei loro confronti sia quelle tentate, anche se il comportamento non è stato posto in essere in modo compiuto, e quelle soltanto prospettate.

In caso di ritorsioni, il predetto D. Lgs. n. 24/2023 prevede un regime di protezione la cui applicazione richiede che la segnalazione, la divulgazione pubblica e la denuncia, effettuate da parte di uno dei soggetti individuati dal legislatore soddisfino alcune condizioni e requisiti; nello specifico, ai fini di godere della protezione:

a) i segnalanti o denuncianti devono ragionevolmente credere, anche alla luce delle circostanze del caso concreto e dei dati disponibili al momento della segnalazione, divulgazione pubblica o denuncia, che le informazioni sulle violazioni segnalate, divulgate o denunciate siano veritiere. Non sono sufficienti invece semplici supposizioni o voci di corridoio così come notizie di pubblico dominio.[9]
b) non rileva invece, ai fini delle tutele, la circostanza che il soggetto abbia segnalato, effettuato divulgazioni pubbliche o denunce pur non essendo certo dell'effettivo accadimento dei fatti segnalati o denunciati e/o dell'identità dell'autore degli stessi o riportando anche fatti inesatti per via di un errore genuino.
c) allo stesso modo, chi effettua una segnalazione, divulgazione pubblica o denuncia ha diritto alla protezione se ha agito sulla base di motivi fondati tali da far ritenere ragionevolmente che le informazioni sulle violazioni segnalate, divulgate o denunciate siano pertinenti in quanto rientranti fra gli illeciti considerati dal legislatore.
d) la segnalazione o la divulgazione pubblica inoltre devono essere effettuate sulla base di quanto previsto dal Capo II del decreto. Si rammenta che nel caso di segnalazioni inviate ad un soggetto diverso da quello competente, quest'ultimo deve trasmetterle senza ritardo al soggetto autorizzato a ricevere e gestire le segnalazioni, dando contestuale notizia della trasmissione alla persona segnalante. Al fine di consentire tale trasmissione tempestiva, il segnalante deve indicare chiaramente nell'oggetto della segnalazione che si tratta di una segnalazione di un whistleblowing.
e) deve esserci uno stretto collegamento tra la segnalazione, la divulgazione pubblica e la denuncia e il comportamento/atto/omissione sfavorevole subito direttamente o indirettamente, dalla persona segnalante o denunciate, affinché questi siano considerati una ritorsione e, di conseguenza, il soggetto possa beneficiare di protezione.

L'art. 17 del D.lgs. n. 24/2023 prevede, inoltre, un regime probatorio di favore per il segnalante; infatti, nell'ambito dei procedimenti giudiziari o amministrativi (anche stragiudiziali) correlati alla segnalazione: nello specifico, viene presunto il carattere ritorsivo dei comportamenti adottati (dalle controparti) a seguito della segnalazione, ritenuti ex lege quale reazioni alla segnalazione o divulgazione o denuncia. Conseguentemente, grava su coloro che hanno posto in essere i suddetti comportamenti, l'onere di dimostrare che gli stessi sono stati motivati da ragioni estranee alla segnalazione o alla divulgazione o alla denuncia (inversione dell'onere della prova); analogo regime di favore è poi previsto, in caso di richiesta risarcitoria, in merito all'accertamento del danno che si presume sia conseguenza della segnalazione o della divulgazione.

non esaustivo. Oltre a quelle espressamente indicate nel D.lgs. n. 24/2023 possono costituire ritorsioni, ad esempio, anche la pretesa di risultati impossibili da raggiungere nei modi e nei tempi indicati; una valutazione della *performance* artatamente negativa; una revoca ingiustificata di incarichi; un ingiustificato mancato conferimento di incarichi con contestuale attribuzione ad altro soggetto; il reiterato rigetto di richieste (ad es. ferie, congedi); la sospensione ingiustificata di brevetti, licenze, etc.

[9] In altri termini ciò che conta è che un soggetto abbia effettuato segnalazioni, divulgazioni pubbliche o denunce, in base ad una convinzione ragionevole (che un illecito stia per verificarsi, ad esempio). Questa rappresenta una salvaguardia essenziale contro segnalazioni dannose o offensive e garantisce che coloro che, hanno deliberatamente e consapevolmente segnalato, divulgato pubblicamente o denunciato informazioni errate, palesemente prive di fondamento o fuorvianti non godano di protezione.

Le misure di protezione di cui al Capo III del D.lgs., n.24/2023, si applicano anche[10]:

a) ai facilitatori[11];
b) alle persone del medesimo contesto lavorativo[12] della persona segnalante[13], di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
c) ai colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
d) agli enti di proprietà della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone[14].

4.4 Nominatività delle Segnalazioni

Le *Segnalazioni* devono essere **nominative** e al segnalante è chiesto di rassegnare i propri estremi identificativi in modo da poter essere riconosciuto e, eventualmente, ricontattato. La normativa richiede, peraltro, che la *Banca/Società del Gruppo* identifichi il soggetto segnalante in qualità di soggetto appartenente al proprio *Personale*.

Il processo adottato e definito nella presente Policy garantisce, comunque, sin dal momento dell'invio della *Segnalazione*, la riservatezza in tutti gli stadi del procedimento; in particolare, l'identità del segnalante non sarà rivelata a terzi. Può, tuttavia, essere necessario comunicare l'identità del segnalante ai soggetti competenti che parteciperanno alle indagini o a eventuali procedimenti giudiziari successivi, eventualmente avviati a seguito della verifica svolta nell'ambito della procedura di segnalazione.

Le **segnalazioni anonime**, ove circostanziate, per ANAC sono equiparate a segnalazioni ordinarie e in tal caso considerate nei propri procedimenti di vigilanza "ordinari". Secondo le Linee Guida Anac,[15] i soggetti del settore pubblico e del settore privato che ricevono le segnalazioni tramite canali interni considerano le segnalazioni anonime alla stregua di segnalazioni ordinarie da trattare secondo i criteri stabiliti nei rispettivi ordinamenti. In ogni caso, il segnalante o il denunciante anonimo, successivamente identificato, che ha comunicato ad ANAC di aver subito ritorsioni può beneficiare della tutela che il decreto garantisce a fronte di misure ritorsive. Gli enti del settore pubblico o privato che ricevono le segnalazioni attraverso canali interni e la stessa Autorità sono, quindi, tenuti a registrare le segnalazioni anonime ricevute e conservare la relativa documentazione non oltre cinque anni decorrenti dalla data di ricezione di tali segnalazioni, rendendo così possibile rintracciarle, nel caso in cui il segnalante, o chi abbia sporto denuncia, comunichi ad ANAC di aver subito misure ritorsive a causa di quella segnalazione o denuncia anonima. Peraltro, fermo restando quanto previsto al precedente punto 3.1, nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.

Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.

10 Cfr. art. 3, comma 5, D.Lgs. n. 24/2023.
11 "Facilitatore": una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata (cfr. art. 2, comma 1, lett. h, D. Lgs. n. 24/2023).
12 "Contesto lavorativo": Le attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di cui all'articolo 3, commi 3 o 4, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile. L'espressione "*persone del medesimo contesto lavorativo del segnalante*" si riferisce, quindi, a persone legate da una rete di relazioni sorte in ragione del fatto che esse operano, o hanno operato in passato, nel medesimo ambiente lavorativo del segnalante o denunciante, ad esempio colleghi, ex-colleghi, collaboratori (cfr. art. 2, comma 1, lett. i, D. Lgs. n. 24/2023).
13 "Persona segnalante": La persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo (cfr. art. 2, comma 1, lett. g, D. Lgs. n. 24/2023).
14 Nel concetto di enti di proprietà si possono ricomprendere: sia i casi in cui un soggetto è titolare di un ente in via esclusiva, sia in compartecipazione maggioritaria con terzi; gli enti presso i quali il segnalante, denunciante o chi effettua una divulgazione pubblica lavorano; enti che operano nel medesimo contesto lavorativo del segnalante, denunciante o di chi effettua una divulgazione pubblica.
15 Le "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne" sono state approvate con Delibera n. 311 del 12 luglio 2023.

In tale ipotesi, viene dato avviso al segnalante con comunicazione scritta delle ragioni della rivelazione dei dati riservati, nonché nelle procedure di segnalazione interna ed esterna di cui al presente capo quando la rivelazione della identità della persona segnalante e delle informazioni di cui al comma 2 è indispensabile anche ai fini della difesa della persona coinvolta. Inoltre, ai sensi del comma 9 dell'art. 12 del D.lgs. n. 24/2023, nelle procedure di segnalazione interna ed esterna di cui al presente capo, la persona coinvolta può essere sentita, ovvero, su sua richiesta, è sentita, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

4.5 Responsabilità del segnalante

Il segnalante non dovrà utilizzare il *Sistema* qui descritto per scopi meramente personali o per effettuare rivendicazioni di lavoro contro superiori gerarchici o la *Banca/Società del Gruppo* in generale, in quanto per tali scopi si deve fare riferimento alle specifiche procedure già in essere.

Eventuali usi impropri o scorretti del *Sistema*, quali le *Segnalazioni* manifestamente opportunistiche, quelle effettuate al solo scopo di danneggiare il segnalato o altri soggetti, nonché ogni altra forma di utilizzo improprio o di intenzionale strumentalizzazione di questo *Sistema*, sono oggetto di provvedimenti sanzionatori e disciplinari.

Il segnalante fornisce informazioni iniziali relative a una ragionevole convinzione, o fondato sospetto, che si è verificata o è in corso un'attività illecita. Il segnalante deve fornire evidenza di atti, fatti o omissioni che possano costituire una violazione di norme disciplinanti l'attività della *Banca/Società del Gruppo* supportandoli da elementi quanto più possibile circostanziati. Tuttavia, non è di responsabilità del segnalante provare la verità delle proprie asserzioni.

L'indagine non potrà, comunque, essere intrapresa senza adeguati riscontri verificabili circa la *Segnalazione* effettuata.

Il segnalante non sarà immune da azioni disciplinari qualora risulti in malafede o sia coinvolto negli illeciti segnalati.

4.6 Canale di Segnalazione Esterna (ANAC)

L'Autorità nazionale anticorruzione (ANAC) ha pubblicato le nuove Linee Guida nonché il Regolamento per la gestione delle segnalazioni esterne e per l'esercizio del potere sanzionatorio dell'ANAC stessa in attuazione del Decreto Legislativo 10 marzo 2023, n. 24[16] che garantiranno, 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. Il segnalante può inviare una **segnalazione esterna** all'ANAC, in presenza di una delle seguenti condizioni ([17]):

a) non è prevista, nell'ambito del contesto lavorativo del segnalante, l'attivazione obbligatoria del canale di segnalazione interna oppure tale canale, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dal D. Lgs. n. 24/2023 per i canali di segnalazione interna;

b) la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;

c) 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;

d) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

[16] Le "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne" sono state approvate con Delibera n. 311 del 12 luglio 2023; il "Regolamento per la gestione delle segnalazioni esterne e per l'esercizio del potere sanzionatorio dell'ANAC in attuazione del Decreto Legislativo 10 marzo 2023, n. 24" è stato adottato con Delibera n. 301 del 12 luglio 2023.
[17] Cfr.art. 6 del D.Lgs. n. 24/2023.

4.7 Divulgazione pubblica

Il segnalante, ai sensi dell'art. 15 del D. Lgs. n. 24/2023, può effettuare direttamente una divulgazione pubblica nei casi in cui:

- 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;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- la persona segnalante 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[18].

4.8 Misure e provvedimenti sanzionatori di competenza dell'ANAC

L'ANAC, in base all'art. 21 del D. Lgs. n. 24/2023 può applicare una serie di sanzioni amministrative pecuniarie ai soggetti, pubblici o privati, in caso di violazione delle regole stabilite dal decreto stesso. In particolare, è prevista una sanzione da 10.000 a 50.000 euro in caso di condotte ritorsive o di comportamenti ostativi all'accertamento della segnalazione o se è stato violato l'obbligo di riservatezza. Sanzioni dello stesso importo sono previste anche per la mancata istituzione di canali di segnalazione o quando non sono state adottate procedure per la gestione delle segnalazioni o queste non sono conformi alle prescrizioni indicate agli articoli 4 e 5 del D.Lgs. n. 24/2023[19].

Per questi comportamenti, nell'ambito del settore privato, l'articolo 21 del decreto dispone che gli enti e le persone giuridiche di cui all'articolo 2, comma 1, lettera q), n. 3, cioè, con meno di 50 dipendenti ma che abbiano istituito un modello organizzativo ai sensi della disciplina di cui al D.Lgs. n. 231/2001, prevedano in esso sanzioni disciplinari nei confronti di coloro che accertano essere responsabili di tali illeciti.

Il medesimo decreto prevede, inoltre, che l'ANAC possa applicare una sanzione pecuniaria da 500 a 2.500 euro nei confronti del segnalante, qualora sia accertata la sua responsabilità per i reati di diffamazione o calunnia nel caso di dolo o colpa grave salvo il caso in cui vi sia stata già una condanna per i medesimi reati o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile.

5. Ruoli e Responsabilità

Di seguito, sono indicati i principali soggetti coinvolti nella gestione del Sistema, attribuendo ad ognuno il relativo ruolo e le connesse responsabilità.

5.1 Organi aziendali

Il Consiglio di Amministrazione della singola *Banca/Società del Gruppo* approva la presente Policy con cui definisce le caratteristiche del *Sistema* adottato.

Il Consiglio di Amministrazione ha il compito di individuare le azioni da intraprendere in funzione dei riscontri ad esso pervenuti ottenuti dall'attività istruttoria.

Inoltre, il Consiglio di Amministrazione:

[18] Cfr. art. 15 del D.Lgs. n. 24/2023.

[19] Si precisa che gli articoli 4 e 5 del D.Lgs. n. 24/2023 hanno ad oggetto, rispettivamente, i Canali di segnalazione interna e la Gestione dei canali di segnalazione interna.

- analizza, valuta e approva l'informativa periodica (relazione annuale del *Responsabile*) sulla gestione del *SISV* anche ai fini di definire eventuali interventi migliorativi del *SISV* e del complessivo sistema dei controlli interni;
- definisce le eventuali modifiche da apportare al *SISV*;
- è informato prontamente delle *Segnalazioni* che per importanza dei fatti possono comportare per la *Banca/Società del Gruppo* l'esposizione a rischi elevati di carattere patrimoniale, operativo o reputazionale.

Il Collegio Sindacale accerta l'adeguatezza del *Sistema* adottato, il corretto assolvimento dei compiti e l'adeguato coordinamento delle funzioni coinvolte, promuovendo gli eventuali interventi correttivi delle carenze e delle irregolarità rilevate. Nell'assolvere a tale compito può avvalersi di strutture operative interne ovvero di consulenti esterni entro il limite di spesa proprio dell'Organismo di Vigilanza.

Il Presidente del Collegio Sindacale riceve, analizza e valuta eventuali *Segnalazioni* che coinvolgono membri del Consiglio di Amministrazione, l'Amministratore Delegato/Direttore Generale e il *Responsabile del SISV*.

Il Collegio Sindacale prende visione della Relazione annuale redatta dal *Responsabile* ed è tempestivamente informato riguardo a eventuali *Segnalazioni* che per importanza dei fatti possono comportare per la *Banca/Società del Gruppo* l'esposizione a rischi elevati di carattere patrimoniale, operativo e reputazionale.

5.2 Responsabile del sistema delle segnalazioni delle violazioni

La Capogruppo individua il *Responsabile* del *Sistema* nel ***Responsabile della Funzione Internal Audit (per la Capogruppo)*** mentre per le società controllate Sevian e Soprarno l'attività è esternalizzata alla Funzione Internal Audit della Capogruppo fermo restando che la Responsabilità del sistema interno di segnalazioni è attribuita all'amministratore indipendente nel rispetto delle disposizioni contenute nell'Allegato 4 del provvedimento BI 5/12/2019 secondo cui le attività di ricezione, esame e valutazione delle segnalazioni possono essere esternalizzate nel rispetto della disciplina in materia di esternalizzazione e il fornitore di servizi riferisce al responsabile del sistema interno di segnalazione che in caso di esternalizzazione non può essere lo stesso soggetto.

Il Responsabile del Sistema interno di segnalazione assicura il corretto svolgimento del procedimento e, nel proprio Rapporto annuale, riferisce direttamente agli *Organi Aziendali* della *Banca/Società del Gruppo* le informazioni oggetto di *Segnalazione*, per la relativa approvazione. In particolare, tale relazione annuale sul corretto funzionamento dei sistemi interni di segnalazione contiene le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, nel rispetto di quanto previsto dalla disciplina sulla protezione dei dati personali.

Il *Responsabile*, in linea con il principio di proporzionalità, può direttamente gestire le fasi di ricezione, esame e valutazione del procedimento di *Segnalazione* ovvero può avvalersi di risorse interne.

Il *Responsabile* assicura la gestione del *Sistema* secondo canoni di riservatezza delle informazioni ricevute e fornisce tempestivamente le informazioni agli *Organi Aziendali* relativamente a particolari casistiche di *Segnalazione* che potrebbero esporre la *Banca/Società del Gruppo* a rilevanti rischi di natura patrimoniale, operativa o reputazionale.

Il *Responsabile* redige una relazione annuale sul corretto funzionamento del *Sistema*, contenente informazioni aggregate sulle risultanze dell'attività svolta a seguito delle *Segnalazioni* ricevute, che viene approvata dal Consiglio di Amministrazione e messa a disposizione al *Personale* sulla Intranet Aziendale.

Al *Responsabile* sono, di norma, indirizzate le *Segnalazioni* da parte del *Personale* attraverso le modalità trasmissive previste nel successivo Capitolo 6.

In caso di indisponibilità del *Responsabile* (per ferie, malattia, missioni, ecc.) questo è sostituito da un delegato da designarsi all'interno della Funzione Internal Audit che assume, per il periodo di sostituzione, ruolo e responsabilità del *Responsabile*.

5.3 Altre Funzioni e Direzioni coinvolte

Le altre Funzioni coinvolte nel processo di gestione delle *Segnalazioni* secondo quanto previsto dalle presenti disposizioni sono:

Amministratore Delegato/Direttore Generale

- assicura l'attuazione del *SISV* in conformità con le norme e in coerenza con la presente Policy;
- adotta le misure opportune a tutela del segnalante eventualmente di concerto con la Direzione Personale previste agli artt. 16 e 19 del D. Lgs. n. 24/2023[20];
- riceve l'informativa del *Responsabile*;
- delibera eventuali provvedimenti e misure sanzionatorie per quanto di competenza.

Funzione Compliance e, nei casi di competenza ratione materiae, la Funzione AML

- supporta il *Responsabile* e, in generale, i soggetti preposti alla ricezione delle *Segnalazioni*, nella verifica dell'ammissibilità della *Segnalazione* con particolare riguardo all'ambito oggettivo (ambito normativo di riferimento per il *SISV*), oltre che con riferimento alle Segnalazioni relative a violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo all'antiriciclaggio.

Data Protection Officer (DPO)

- esamina e verifica il modello e il funzionamento dello stesso, al fine di valutare la rispondenza dello stesso alla normativa vigente in materia di privacy.

Responsabile del Personale

- assicura l'attività formativa, di concerto con il *Responsabile*;
- adotta le misure opportune a tutela del segnalante eventualmente di concerto con l'Amministratore Delegato/Direttore Generale;
- pone in essere eventuali provvedimenti e misure sanzionatorie deliberate dagli Organi competenti.

Qualora si configurino comportamenti sanzionabili sul piano disciplinare, il Responsabile del Personale pone in essere quanto necessario.

-

5.4 Controllo sul sistema di segnalazione delle violazioni

I controlli sul *Sistema* sono assicurati

- dal *Responsabile* che vigila nel continuo sul corretto funzionamento del *SISV* e relaziona annualmente gli *Organi Aziendali* circa il suo funzionamento;
- dalla Funzione Compliance che, in qualità di presidio di secondo livello con riguardo al rischio di non conformità alle norme, è responsabile della gestione del rischio di non conformità del *SISV* alle norme applicabili;
- dal Collegio Sindacale che vigila sull'adeguatezza, completezza, funzionalità e affidabilità del *SISV* avvalendosi dell'eventuale ausilio di risorse interne ovvero di consulenti esterni indipendenti.

5.5 Rapporti con l'Organismo di Vigilanza

20 L'art. 16 e l'art. 19 del D. Lgs. n. 24/2023 hanno ad oggetto, rispettivamente, le "Condizioni per la protezione della persona segnalante" e la "Protezione dalle ritorsioni".

Qualora nel corso dell'istruttoria si rilevino presunte o accertate violazioni riferibili ai reati di cui al D. Lgs. n. 231/2001 sarà fornita opportuna informativa all'Organismo di Vigilanza nel rispetto dei principi di riservatezza e confidenzialità delle informazioni del segnalante e dell'eventuale segnalato.

5.6 Trattamento dei dati personali nelle segnalazioni whistleblowing

In merito al trattamento dei dati personali per le segnalazioni whistleblowing, il titolare del trattamento è:

- Gruppo Bancario Ifigest, P.zza Santa Maria Soprarno 1 – 50125 Firenze;

Nel rispetto degli adempimenti previsti dalla normativa in materia di protezione dei dati personali, i titolari del trattamento sopraindicati hanno provveduto, singolarmente, a designare la società _____, fornitrice del software per le segnalazioni sul whistleblowing, responsabile del trattamento dei dati personali ai sensi dell'art. 28 del GDPR ed i Responsabili della Funzione Internal Audit, quali soggetti autorizzati al trattamento dei dati per le segnalazioni in oggetto.

Il Titolare del trattamento può, inoltre, avvalersi del *Data Protection Officer* (DPO) inteso come la persona fisica incaricata di informare e consigliare il Titolare, nonché i dipendenti, in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali.

I dati personali dei Segnalanti, dei Segnalati e di tutti i soggetti coinvolti nella Segnalazione sono trattati in conformità con la normativa vigente in materia di protezione dei dati personali.

In particolare, si evidenza in tale contesto che:

- le attività di trattamento sottese alla gestione della Segnalazione sono svolte nel rispetto dei principi dettati dall'art. 5 GDPR;
- il soggetto Segnalante - e nei limiti e nei modi previsti dalla normativa - il soggetto segnalato e tutte le persone coinvolte- riceveranno una informativa di cui agli art. 13 e 14 del GDPR che specifica le finalità e modalità del trattamento dei dati personali e il periodo di conservazione degli stessi, le condizioni di liceità su cui si basa il trattamento, le categorie di destinatari a cui possono essere trasmessi i dati nell'ambito della gestione della Segnalazione e i diritti riconosciuti al Segnalante dalla Policy;
- il sistema di segnalazione prevede che i dati personali trattati (potenzialmente, anche i dati particolari di cui all'art. 9 GDPR) siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono raccolti.

Inoltre, i dati personali saranno trattati per il tempo necessario per il raggiungimento delle finalità che ne giustificano la raccolta (es.: valutazione e gestione della segnalazione); una volta esaurita la finalità di trattamento, i dati personali saranno conservati sulla base dei criteri e per i periodi indicati all'interno dell'informativa sul trattamento dei dati resa all'interessato e successivamente cancellati o anonimizzati;

- il titolare ha messo in atto le misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali, in conformità con la normativa vigente, sia in fase di trasmissione della Segnalazione, sia in fase di gestione e archiviazione della Segnalazione, e al fine di limitare i rischi connessi al trattamento di tali dati il Titolare ha posto in essere una valutazione di impatto ai sensi della normativa
- l'esercizio dei diritti da parte del Segnalante o del Segnalato (soggetti "interessati" ai sensi della normativa in materia di protezione dei dati personali), in relazione ai dati personali trattati nell'ambito del processo di Whistleblowing, possono essere limitati, ai sensi e per gli effetti di cui all'articolo 2-undecies del D.lgs. 196/2003 e s.m.i., nel caso in cui da un tale esercizio possa derivarne un pregiudizio effettivo e concreto ad altri interessi tutelati da specifiche disposizioni normative, con la precisazione che in nessuna circostanza può essere permesso al Segnalato di avvalersi dei propri diritti per ottenere informazioni sull'identità del Segnalante;
- l'accesso ai dati personali viene concesso solamente ai soggetti autorizzati e abilitati alla ricezione di tale tipologia di Segnalazioni, limitando il trasferimento delle informazioni riservate e dei dati personali soltanto quando ciò risulta necessario e nei casi previsti dalla legge;

– i dati personali vengono conservati limitatamente ai termini appropriati e proporzionati al fine di consentire l'esecuzione della Procedura di Whistleblowing.

6. Processo di gestione delle segnalazioni di violazione

Il processo di segnalazione interna delle violazioni della *Banca/Società del Gruppo* è strutturato nelle fasi di seguito descritte:

6.1 Canale e modalità di trasmissione delle segnalazioni

Canali di comunicazione

Le fasi di invio, ricezione e istruttoria si avvalgono del relativo Canale gestito attraverso un'apposita Piattaforma (_____) - accessibile attraverso l'apposito link presente nei siti istituzionali delle singole Banche/Società del Gruppo - in grado di soddisfare i requisiti in tema di riservatezza di cui all'art. 4, comma 1, D.Lgs. n. 24/2023.

La *Banca/Società del Gruppo* ha individuato quale soggetto preposto alla ricezione, esame e valutazione della *Segnalazione* il ***Responsabile della Funzione Internal Audit*** nel presupposto che possa soddisfare i seguenti requisiti:

a) non sia gerarchicamente o funzionalmente subordinato all'eventuale soggetto segnalato;

b) non sia esso stesso il presunto responsabile della violazione;

c) non abbia un potenziale interesse correlato alla segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio.

Qualora non sia assicurato il rispetto di tali requisiti la *Banca/Società del Gruppo* ha previsto, nella predetta Piattaforma, la possibilità di indirizzare le *Segnalazioni* anche al Presidente del Collegio Sindacale.

Le modalità di utilizzo della Piattaforma sono riportate nell'apposita documentazione operativa.

Modalità trasmissive

La Piattaforma adottata è in grado di assicurare la riservatezza e la protezione delle informazioni trasmesse; in particolare, essa garantisce:

– la riservatezza dell'identità della persona segnalante;

– la riservatezza della persona coinvolta e della persona comunque menzionata nella segnalazione;

– la riservatezza del contenuto della segnalazione e della relativa documentazione.

A seguito dell'inserimento della Segnalazione, la Piattaforma inoltra automaticamente un avviso al *Responsabile* del SISV per l'avvio delle successive fasi istruttorie.

Al *Responsabile*, altresì, possono essere rappresentate *Segnalazioni* verbali tramite colloquio personale; in tale caso, la *Segnalazione* dovrà sempre essere verbalizzata e sottoscritta dal segnalante.

Il *Responsabile* dovrà svolgere le seguenti attività:

1) **rilasciare alla persona segnalante avviso di ricevimento** della segnalazione **entro sette giorni** dalla data di ricezione (attività gestita automaticamente tramite la Piattaforma utilizzata);
2) mantenere le interlocuzioni con la persona segnalante e poter richiedere a quest'ultima, se necessario, integrazioni (attività supportata anch'essa dalla Piattaforma in uso);
3) dare diligente seguito alle segnalazioni ricevute;
4) **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. La Piattaforma in uso supporta Responsabile attraverso specifiche funzioni di notifica/alerting.

6.2 Ricezione della segnalazione

Il segnalante deve necessariamente essere riconosciuto come soggetto appartenente al *Personale* della *Banca/Società del Gruppo*, così come definito nel precedente paragrafo 4.2.

Il *Responsabile* ha l'obbligo di garantire la confidenzialità delle informazioni ricevute, anche in merito all'identità del segnalante, e accerta che la *Segnalazione* ricevuta possegga i contenuti richiesti. In caso negativo contatta il segnalante, tramite Piattaforma, per richiedere le informazioni mancanti; nel caso in cui queste non siano fornite e ciò impedisca la prosecuzione dell'indagine, il *Responsabile* procede all'archiviazione della *Segnalazione* e delle connesse informazioni dopo aver tenuto traccia della stessa ai soli fini statistici.

La Piattaforma garantisce la protocollazione delle singole segnalazioni e della documentazione allegata.

6.3 Segnalazioni "Telefoniche e orali"

Il D. Lgs.n. 24/2023 prevede la possibilità di effettuare segnalazioni orali "*avvalendosi di linee telefoniche o sistemi di messaggistica vocale o, ancora, mediante un incontro diretto fissato entro un termine ragionevole*". Il numero telefonico dedicato è il 3371352089

Nel caso in cui per la segnalazione si utilizzi una linea telefonica registrata, o altro sistema di messaggistica vocale, la segnalazione, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto, oppure mediante trascrizione integrale. In caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Se per la segnalazione si utilizza una linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato, la segnalazione è documentata per iscritto mediante resoconto dettagliato della conversazione a cura del personale addetto. La persona segnalante può verificare, rettificare e confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il Responsabile del SISV, essa, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante stesura di apposito verbale sottoscritto dal segnalante.

6.4 Esame della segnalazione

L'esame della *Segnalazione* è effettuato a partire dalle informazioni acquisite nell'ambito dell'attività di ricezione della *Segnalazione*. Il *Responsabile* avvalendosi del supporto di eventuali risorse interne e/o esterne allo scopo preposte, effettua l'esame della documentazione acquisita e procede alle verifiche del caso.

I soggetti a tale scopo deputati, verificano la sussistenza dei requisiti di ammissibilità, svolgono un'analisi preliminare della *Segnalazione* per valutarne le caratteristiche, i tempi e le modalità di indagine nonché i potenziali impatti e, infine, svolgono un'attività istruttoria.

Lo scopo dell'**analisi preliminare** non è quello di giungere a una conclusione definitiva sul fatto accaduto o sulle responsabilità, bensì quello di fare una "verifica di ammissibilità" della *Segnalazione* nonché una valutazione preliminare delle prove a disposizione per determinare se vi siano elementi sufficienti per giustificare un'ulteriore istruttoria e il grado di rilevanza/rischiosità.

La "verifica di ammissibilità" deve stabilire se la *Segnalazione* possegga tutte le caratteristiche necessarie per renderla ammissibile; in particolare devono essere verificate l'ammissibilità del segnalante, l'ammissibilità dell'atto/fatto segnalato e la presenza di eventuali conflitti per il soggetto preposto all'esame.

I risultati dell'**analisi preliminare** devono essere registrati dal *Responsabile* in un apposito documento (Risultanze dell'Analisi preliminare caricato nella Piattaforma Whistleblowing) nel quale si stabilisce se si debba o meno procedere ad una formale Istruttoria e le ulteriori indagini che al momento paiono da condurre.

A tal fine, si dovranno considerare, tra gli altri, i seguenti fattori:

- informazioni fornite a corredo della *Segnalazione*;
- attuali procedure in vigore attinenti ai fatti segnalati;
- *Segnalazioni* precedenti aventi lo stesso oggetto e già esaminate;
- fatti o situazioni, rispetto ai quali è già in corso un'indagine da parte di pubbliche autorità.

Sulla base delle risultanze dell'Analisi preliminare, nel documento predetto si dovrà anche stabilire se la *Segnalazione* possa essere ritenuta "rilevante" e, come tale, debba essere avviata una "procedura d'urgenza" (Cfr. § 6.5 - *Gestione delle segnalazioni rilevanti*).

L'**Istruttoria** ha, infine, lo scopo di esplorare in dettaglio i fatti/atti denunciati nella *Segnalazione*, accertando l'esistenza o acquisendo prove a supporto degli atti o fatti denunciati e delle responsabilità connesse. L'attività istruttoria deve anche raccogliere elementi utili per stabilire l'effettiva rilevanza e portata per la *Banca/Società del Gruppo* delle violazioni segnalate. Allo scopo può essere previsto lo svolgimento di ogni attività ritenuta opportuna anche mediante il coinvolgimento delle eventuali Funzioni aziendali competenti e/o del soggetto segnalante.

Qualora la segnalazione sia classificata come "non ammissibile" viene data informativa al segnalante tramite Piattaforma.

6.5 Gestione delle segnalazioni rilevanti

Il *Sistema* deve consentire di identificare e comunicare senza indugio agli *Organi Aziendali* le *Segnalazioni* ritenute "rilevanti".

Per "segnalazioni rilevanti" sono da intendersi, oltre a quelle che riguardano membri degli *Organi Aziendali,* le *Segnalazioni* per le quali, anche solo dopo una prima analisi preliminare, si ritenga possibile una o più delle seguenti situazioni:

- un sensibile impatto in bilancio;
- un significativo impatto reputazionale;
- violazione del Modello Organizzativo ex D.Lgs. n. 231/2001;
- una deficienza/carenza significativa del Sistema dei Controlli Interni.

In caso di "segnalazioni rilevanti", il *Responsabile* informa tempestivamente il Presidente del Collegio Sindacale,anche ai fini di un'eventuale convocazione del Consiglio.

In caso di "segnalazioni rilevanti" o, comunque, afferenti fatti segnalati sui quali sono in corso di svolgimento indagini da parte di Autorità Pubbliche, nelle attività di esame e valutazione deve essere coinvolta la Direzione Affari Legali e Societari.

In caso di "segnalazioni rilevanti", nonché in ogni situazione ove sia ipotizzabile che siano ancora in corso azioni illecite, sono applicate apposite **procedure d'urgenza** che consentano una veloce definizione e attuazione di interventi per la loro risoluzione ovvero per la mitigazione degli effetti.

Il *Responsabile* stabilisce, a fronte dei riscontri avuti (Analisi preliminare o Istruttoria), se sia opportuno avviare una procedura d'urgenza, motivandone le ragioni in modo chiaro. In tal caso il *Responsabile* attiva le opportune misure di urgenza sulla base delle istruzioni ricevute dagli *Organi Aziendali* preventivamente informati; dette misure possono essere adottate anche prima che il segnalato sia informato della *Segnalazione*. Lo svolgimento del processo deve, comunque, proseguire seguendo il normale iter e le responsabilità per esso definite.

6.6 Valutazione della segnalazione

Nella fase di valutazione può essere, eventualmente, necessario procedere ad ulteriori accertamenti ed alla raccolta di ulteriori informazioni. Nel processo valutativo il *Responsabile* può avvalersi della collaborazione di altre figure di riferimento del *SISV* all'interno del Gruppo (Responsabile Compliance, membri del Collegio Sindacale, Responsabile Personale).

Prima della conclusione di questa fase, fatti salvi i casi di procedura d'urgenza, il segnalato deve essere informato dell'oggetto della *Segnalazione* a suo carico, per gli effetti di cui al precedente par. 4.3 ("Tutela del segnalante"), e può controdedurre entro il termine indicato alla comunicazione.

Al termine di questa fase il *Responsabile* effettua, un apposito documento ("Risultanze della Istruttoria e Valutazione") la descrizione dei fatti emersi e la loro valutazione (anche alla luce delle eventuali controdeduzioni del segnalato) definendone la rilevanza, i possibili effetti/conseguenze per la *Banca/Società del Gruppo*, nonché chiarendo le motivazioni che hanno condotto alla valutazione stessa.

Detto documento è tempestivamente trasmesso al Consiglio di Amministrazione per le valutazioni e decisioni conseguenti.

Alla segnalazione deve essere fornito riscontro **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, decorrente dalla presentazione della segnalazione[21].

6.7 Azioni

La fase decisoria spetta al Consiglio di Amministrazione con possibilità di delega all'Amministratore Delegato/Direttore Generale nei limiti consentiti dallo Statuto ([22]). Gli Organi competenti potranno:

a) avviare i procedimenti disciplinari, o altre decisioni utili, nei confronti dei soggetti segnalati riconosciuti responsabili;

b) avviare la procedura sanzionatoria nei confronti del segnalante che abbia agito con dolo e/o colpa grave;

c) non effettuare alcuna azione e disporre l'archiviazione della *Segnalazione*.

La decisione finale viene comunicata al segnalante, qualora lo stesso abbia manifestato il desiderio di conoscerla, al segnalato, in modo riservato, e al suo *Responsabile.* La stessa deve successivamente essere oggetto di archiviazione protetta.

In considerazione dei riscontri ottenuti, qualora lo si ritenga opportuno ovvero in caso di emersione di fatti e circostanze che per legge devono essere oggetto di denuncia presso l'autorità di competenza, possono essere attivate ulteriori azioni quali:

- segnalazioni alla competente autorità giudiziaria;
- segnalazione agli Organi di Vigilanza;
- definizione di eventuali azioni di prevenzione e di mitigazione.

La *Banca/Società del Gruppo* valuta, anche nel caso in cui gli atti/fatti siano accertati ma non ascrivibili a soggetti puntualmente identificati, eventuali misure per la mitigazione dei rischi connessi e per prevenire il ripetersi delle violazioni occorse.

6.8 Reporting

21 Cfr. art. 5 del D.Lgs. n. 24/2023.

[22] In caso di segnalazione riguardante un membro del CdA lo stesso deve ovviamente astenersi dal partecipare alla fase decisoria in esame.

l processi di valutazione delle *Segnalazioni* formano oggetto di apposito rapporto annuale al Consiglio di Amministrazione. L'attività di reporting contiene una sintesi dei maggiori dati statistici aggregati (numero segnalazioni, numero di provvedimenti sanzionatori adottati con distinzione dei provvedimenti disciplinari applicati, numero soggetti segnalati, Funzioni aziendali coinvolte ecc.) secondo lo schema tipo contenuto nell'Allegato A – Schema dell'informativa annuale sul *SISV*.

Tale relazione è approvata dal Consiglio di Amministrazione e messa a disposizione del *Personale* sulla Intranet Aziendale.

6.9 Archiviazione, conservazione e tracciabilità delle segnalazioni

Il *Responsabile* assicura:

- la tracciabilità delle *Segnalazioni* e delle relative attività di analisi, valutazione e decisione;
- la corretta conservazione della documentazione inerente alle *Segnalazioni* e le relative attività di verifica.

Le attività di conservazione, tracciabilità ed archiviazione delle *Segnalazioni* devono essere effettuate nel rispetto dei requisiti di confidenzialità e riservatezza previsti dalla normativa in materia di protezione dei dati personali.

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, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del presente decreto e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018[23].

Ai fini della conservazione delle segnalazioni orali, si applicano i commi 2, 3 e 4 dell'art. 14 del D.Lgs. n. 24/2023 (cfr. anche par. 6.3).

6.10 Formazione

Allo scopo di assicurare al *Sistema* la necessaria efficacia, è essenziale che i principi stabiliti da questa Policy siano diffusi a tutti i destinatari nonché recepiti in idonee procedure operative che forniscano una chiara descrizione delle attività previste e degli strumenti allo scopo utilizzati.

La *Banca/Società del Gruppo* si impegna ad assicurare la diffusione della presente Policy a tutto il *Personale* attraverso la pubblicazione sulla Intranet Aziendale. I contenuti della presente Policy, inoltre, saranno portati a conoscenza di ciascun dipendente all'atto dell'assunzione, nonché dei soggetti interessati ex D.lgs. n. 24/2023.

Al personale è data specifica informazione circa il fatto che la disposizione di legge in base alla quale il presunto responsabile ha il diritto di ottenere, tra l'altro, l'indicazione dell'origine dei dati personali (ai sensi di quanto previsto dalla normativa vigente in materia di protezione dei dati personali), non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.

A coloro che, ai fini della presente Policy, rientrano nella categoria *Personale* si applicano gli stessi requisiti formativi ed informativi appena descritti ancorché, in relazione al tipo e durata del rapporto con la *Banca/Società del Gruppo*, possano essere oggetto di modalità e tempistiche distinte rispetto al Personale dipendente.

Per i collaboratori esterni deve anche essere definita un'apposita clausola contrattuale, da inserire nei contratti o accordi che disciplinano la prestazione di attività o collaborazione degli stessi a favore della *Banca/Società del Gruppo*, che stabilisca l'assoggettamento di tali collaboratori esterni alla disciplina interna in tema di "segnalazione delle violazioni".

6.11 Valutazione del sistema interno di segnalazione delle violazioni

[23] Cfr. art. 14 del D.Lgs. n. 24/2023.

La Funzione Compliance fornisce le proprie valutazioni e considerazioni di competenza in merito alla conformità del *SISV* alla normativa di riferimento vigente che trasmette al *Responsabile*, per le valutazioni che quest'ultimo deve effettuare nell'ambito della propria relazione annuale sul corretto funzionamento dei sistemi di segnalazione (cfr. il precedente par. 5.2).

La valutazione di adeguatezza deve considerare i seguenti aspetti di impianto:

- conformità della regolamentazione interna e conformità rispetto alle norme esterne applicabili;
- chiarezza e completezza delle istruzioni operative per l'utilizzo del sistema da parte del *Personale*;
- esistenza di adeguate procedure interne formalizzate a supporto dei soggetti coinvolti nel processo;
- esistenza di adeguate attività formative e di campagne di sensibilizzazione del *Personale*.

Il *Responsabile*, se del caso anche con il supporto della Funzione Compliance, coinvolge il DPO per la verifica in merito esistenza di adeguate procedure per la gestione del trattamento dei dati personali.

La Funzione AML viene coinvolta per i profili di competenza, relativi all'adeguatezza del modello ai fin di rispettare la normativa di riferimento.

Al fine di accertare il corretto funzionamento del *Sistema* il *Responsabile* deve svolgere verifiche sia in merito all'effettivo rispetto dell'impianto definito, sia con riferimento alla sua reale efficacia. In particolare, devono essere valutati i seguenti aspetti:

- piena e corretta applicazione delle disposizioni interne in materia;
- rispetto delle tempistiche previste;
- rispetto dei principi di riservatezza e protezione delle informazioni e, in particolare, dei dati personali del segnalante e del segnalato;
- effettiva e corretta applicazione dei principi di tutela del segnalante e del segnalato;
- adeguata conservazione delle informazioni;
- adeguatezza dell'attività formativa.

L'analisi e la valutazione del *SISV* possono essere svolte, oltre che a cura del *Responsabile*, anche a fronte di specifiche richieste di verifica da parte del Collegio Sindacale che, allo scopo, può avvalersi di risorse interne non coinvolte nel processo ovvero di idonei consulenti esterni nel limite di spesa assegnato al Collegio Sindacale nella qualità di Organismo di Vigilanza.

La relazione del *Responsabile* sul corretto funzionamento dei sistemi interni di segnalazione viene messa a disposizione del personale, mediante pubblicazione sull'intranet aziendale.

7. Misure e provvedimenti sanzionatori

Tutti i dipendenti sono tenuti ad osservare le disposizioni contenute nella presente Policy. Un eventuale mancato rispetto o violazione delle regole qui riportate può comportare l'attivazione, da parte del datore di lavoro, di iniziative di carattere disciplinare, con le procedure e le garanzie previste dalla legge, dai contratti e dai regolamenti aziendali tempo per tempo vigenti, fatte salve eventuali responsabilità di natura civile, amministrativa e/o penale.

Nel rapporto che regola il contratto dei collaboratori esterni sono previste le misure che la *Banca/Società del Gruppo* può adottare in caso di violazioni previste dalla presente Policy; per i contratti in essere alla data di approvazione della presente Policy, quanto previsto dal precedente capoverso si applica in sede di rinnovo dei contratti stessi.