



PROCEDURA SEGNALAZIONE DELLE VIOLAZIONI (WHISTLEBLOWING)

- UNITÀ ORGANIZZATIVE: **AMMINISTRATORE DELEGATO/ DIRETTORE GENERALE**
- RESPONSABILE: **FUNZIONE COMPLIANCE**
- DESTINATARI: **CONSIGLIO DI AMMINISTRAZIONE/ COLLEGIO SINDACALE / DIPENDENTI / COLLABORATORI**
- STORIA DEL DOCUMENTO:

DATA	VERSIONE	APPROVAZIONE
20/12/2023	1.0/2023	Consiglio di Amministrazione (20 dicembre 2023)
28/03/2019	0.0/2019	Consiglio di Amministrazione (28 marzo 2019)



INDICE

I. ASPETTI GENERALI DEL PROCESSO DI SEGNALAZIONE DELLE VIOLAZIONI	3
1. Premessa	3
1.2 Ambito di applicazione	4
1.3 Definizione	4
1.4 Oggetto della Segnalazione	6
II. DESCRIZIONE DEL PROCESSO RELATIVO A SEGNALAZIONI INTERNE	8
2. Gli elementi e le caratteristiche della Segnalazione	8
2.1 Soggetto destinatario della Segnalazione.....	9
2.2 La registrazione della Segnalazione	9
2.3 Fase di Istruttoria	10
2.4 Fase di gestione della segnalazione	10
III. PROTEZIONE, SANZIONI, CANALI DI SEGNALAZIONE, TRATTAMENTO DATI	11
3. Misure di protezione.....	11
3.1 Sistema sanzionatorio.....	12
3.2 Segnalazione di violazioni alla Banca d'Italia e alla Consob.....	12
3.3 Divulgazione pubblica	13
3.4 Formazione del personale	13
3.5 Trattamento dei dati personali e conservazioni della documentazione	14



I. ASPETTI GENERALI DEL PROCESSO DI SEGNALAZIONE DELLE VIOLAZIONI

1. Premessa

Lo scopo della presente Procedura è quello di dotare **CAMPERIO SIM S.P.A** (di seguito, la “**SIM**” o la “**Società**”) di un documento che descriva e regolamenti il processo di trasmissione, ricezione, analisi e gestione delle Segnalazioni (cd. **Whistleblowing**) su informazioni, adeguatamente circostanziate, riferibili dai collaboratori o da altri soggetti legati contrattualmente alla Società (c.d. “**whistleblower**”). La procedura fornisce ai whistleblower chiare indicazioni operative riguardo all’oggetto, ai contenuti, ai destinatari e alle modalità di trasmissione delle segnalazioni, nonché le forme di tutela che vengono loro garantite dalla Società agli stessi whistleblower.

La Procedura è finalizzata a dare attuazione alle disposizioni del Decreto Legislativo 10 marzo 2023 n. 24 di esecuzione della Direttiva (UE) 2019/1937 (“**Direttiva**”), 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, (cd. disciplina Whistleblowing). Tale decreto stabilisce la regolamentazione dei canali di segnalazione e delle tutele accordate ai segnalanti, ovvero coloro che segnalano informazioni di violazioni di disposizioni normative nazionali o dell’Unione Europea che ledono l’interesse pubblico o l’integrità dell’amministrazione pubblica o dell’ente privato, di cui siano venuti a conoscenza in un contesto lavorativo pubblico o privato.

L’uso dello strumento di whistleblowing contribuisce ad individuare e combattere la corruzione e qualsiasi forma di illecito, a tutelare la Società da danni economici e all’immagine, a diffondere la cultura dell’etica, della legalità e della trasparenza nonché a rafforzare il sistema dei controlli interni e della gestione dei rischi.

Per quanto non espressamente indicato dalla presente Procedura resta integralmente applicabile quanto previsto dal suddetto Decreto Legislativo.

Infine, gli articoli 4-undecies e 4-duodecies del TUF, che recepiscono le previsioni della Direttiva MiFID II e del Regolamento MiFIR, prevedono che la Segnalazione dei Comportamenti Illegittimi possa avvenire, a seconda dei casi, mediante:

- i. Segnalazione interna alla Società (c.d. “whistleblowing interno”) e/o
- ii. Segnalazione esterna alla Società stessa e indirizzata alle Autorità di Vigilanza (c.d. “whistleblowing esterno”).

Il documento si applica nell’ambito di tutte le attività operative della SIM ha, altresì, lo scopo di disciplinare le modalità di accertamento della validità e fondatezza delle segnalazioni e, conseguentemente, di intraprendere le azioni correttive e disciplinari opportune a tutela della stessa.

- Fonti normative
- Decreto legislativo 10 marzo 2023, n. 24, recante “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. (Decreto whistleblowing)”;
- 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 (cd. *Whistleblowing*);

- Regolamento (UE) n. 2016/679 (Regolamento Generale sulla Protezione dei Dati – GDPR);
- Decreto Legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali e successive modifiche ed integrazioni, tra cui il Decreto Legislativo 10 agosto 2018, n. 101, nonché le collegate disposizioni legislative);
- Provvedimento Banca d'Italia del 26 marzo 2019, recante disposizioni attuative in materia di organizzazione, procedure e controlli interni per evitare il coinvolgimento degli intermediari finanziari in fenomeni di Riciclaggio e di Finanziamento del terrorismo (di seguito, “Provvedimento in materia di organizzazione”);
- D.Lgs. 24 febbraio 1998, n. 58, Testo unico delle disposizioni in materia di intermediazione finanziaria, ai sensi degli articoli 8 e 21 della legge 6 febbraio 1996, n. 52 (di seguito anche “TUF”);
- Direttiva 2013/36/UE del Parlamento Europeo e del Consiglio del 26 giugno 2013 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (di seguito anche “CRD IV”);
- Legge 30 novembre 2017, n. 179, recante “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” (c.d. “Legge sul *Whistleblowing*”);
- Linee guida relative alle procedure per la presentazione e gestione delle segnalazioni esterne, predisposte da A.N.A.C. in attuazione del Decreto Legislativo n. 24 del 2023 (testo approvato con Delibera n. 311 del 12 luglio 2023).

1.2 Ambito di applicazione

La presente procedura disciplina la gestione delle Segnalazioni poste in essere da parte de seguenti soggetti:

- i membri del Consiglio di Amministrazione e del Collegio Sindacale;
- tutti i dipendenti;
- i soci;
- i consulenti e i collaboratori anche occasionali;
- qualsiasi persona che presti servizio per la Società, inclusi i lavoratori autonomi e i liberi professionisti;
- i volontari e i tirocinanti (retribuiti e non);
- i fornitori di servizi in base ad un contratto e/o lettera di incarico;

di seguito congiuntamente i “Destinatari”.

1.3 Definizione

Ai fini della presente Procedura si intende per:

- **Canali di segnalazione:** sistemi diversificati previsti dal Decreto per la presentazione delle Segnalazioni: (i) Canale interno; (ii) Canale esterno presso le autorità di Vigilanza (iii) Divulgazione pubblica;
- **Canale interno per la segnalazione:** piattaforma informatica denominata “**Whistleblowing**” utilizzata dalla SIM ed utilizzabile per effettuare le Segnalazioni interne;



- **Comunicazioni esterne:** segnalazioni fatte dal personale di una SIM alle Autorità di Vigilanza, come Banca d'Italia e Consob, riguardo a violazioni delle norme finanziarie, del TUF (Testo Unico della Finanza), e di atti dell'Unione europea applicabili nelle stesse materie.
- **Contesto lavorativo:** le attività lavorative o professionali, presenti o passate, svolte dal Personale della SIM o da Terzi nell'ambito dei rapporti giuridici da questi instaurati con la SIM;
- **Divulgazione pubblica:** rendere 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, ai sensi dell'art. 15, comma 1, del d.lgs. n. 24/2023;
- **Facilitatore:** la persona fisica che assiste il Segnalante nel processo di Segnalazione e che opera nel medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- **Funzione Ricevente:** Funzione incaricata alla ricezione del sistema di segnalazione interno delle violazioni, che coincide con il Responsabile della Funzione Compliance della SIM;
- **Informazioni sulle violazioni:** informazioni, adeguatamente circostanziate, compresi i fondati sospetti, riguardanti violazioni conseguenti a comportamenti, atti od omissioni commessi o che, sulla base di elementi concreti, potrebbero essere commessi nonché elementi riguardanti condotte, anche omissive, volte ad occultare tali violazioni. Rientrano anche le informazioni su violazioni acquisite nell'ambito di un rapporto giuridico non ancora iniziato o nel frattempo terminato, qualora dette informazioni siano state acquisite nell'ambito del contesto lavorativo, compreso il periodo di prova, oppure nella fase selettiva o precontrattuale;
- **Persona coinvolta/Segnalato:** la persona fisica o giuridica menzionata nella Segnalazione effettuata tramite il canale interno o esterno, denuncia, Divulgazione pubblica, come soggetto a cui la violazione è attribuita o comunque riferibile;
- **Personale:** coloro che sono legati alla SIM da un rapporto di lavoro subordinato o di prestazione occasionale nonché i Vertici aziendali e i componenti degli organi sociali.
- **Segnalante:** la persona che effettua una Segnalazione tramite il canale di Segnalazione interno o esterno, denuncia, Divulgazione pubblica;
- **Segnalazione:** la comunicazione, scritta o orale, di informazioni riferibili al Personale della SIM e/o a Terzi su violazioni di normative nazionali e di diritto dell'Unione europea.
- **Segnalazione anonima:** Segnalazione in cui le generalità del Segnalante non sono esplicitate né risultano identificabili in maniera univoca;
- **Segnalazione circostanziata:** Segnalazione in cui le informazioni/asserzioni sono caratterizzate da un grado di dettaglio sufficiente, almeno astrattamente, a far emergere circostanze e fatti precisi e concordanti e relazionate a contesti determinati, nonché a consentire di identificare elementi utili ai fini della verifica della fondatezza della Segnalazione stessa (ad esempio, elementi che consentono di identificare il soggetto che ha posto in essere i fatti segnalati, il contesto, il luogo e il periodo temporale delle circostanze segnalate, valore, cause e finalità delle condotte, anomalie relative al sistema di controllo interno, documentazione a supporto, ecc.). Nell'ambito delle Segnalazioni circostanziate si distinguono le informazioni/asserzioni:
 - i. “verificabili”, qualora in base ai contenuti della Segnalazione sia possibile in concreto svolgere verifiche in ambito aziendale sulla fondatezza, nei limiti delle attività e con gli strumenti di analisi a disposizione di Audit;
 - ii. “non verificabili”, qualora sulla base degli strumenti di analisi a disposizione, non risulta possibile svolgere verifiche sulla fondatezza della Segnalazione. Le verifiche su circostanze e valutazioni riconducibili ad elementi intenzionali e/o soggettivi risentono dei limiti propri delle attività di Audit e dei relativi strumenti a disposizione;
- **Segnalazione esterna:** la comunicazione, scritta od orale, di Informazioni sulle violazioni



effettuata dal Segnalante tramite il canale di segnalazione esterno attivato dalle Autorità di Vigilanza (Consob e Banca d'Italia).

- **Segnalazione interna:** la comunicazione, scritta o orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interno;
- **Segnalazione relativa a fatti rilevanti:**
 - i. Segnalazione che riguarda i vertici aziendali e i componenti degli organi sociali della SIM;
 - ii. Segnalazione su anomalie operative aziendali e/o illeciti e/o frodi e/o abusi per le quali, all'esito delle verifiche preliminari, sia apprezzabile per la SIM un impatto qualitativo significativo sul bilancio (in termini di tematiche di contabilità, revisione legale dei conti, controlli interni sull'informativa finanziaria);
- **Terzi:** le persone fisiche o giuridiche, diverse dal Personale della SIM, che intrattengono, a vario titolo, rapporti di lavoro, di collaborazione o d'affari con la SIM, ivi compresi - a titolo non esaustivo - i clienti, i partner, i fornitori, i lavoratori autonomi o titolari di rapporti di collaborazione, i liberi professionisti, i consulenti, i promotori e intermediari, i tirocinanti (retribuiti o non retribuiti), ovvero chiunque sia legittimo portatore di interesse nei confronti dell'attività aziendale della SIM.

1.4 Oggetto della Segnalazione

Il Decreto Legislativo n. 24/2023 stabilisce che sono oggetto di segnalazione, divulgazione pubblica o denuncia le informazioni relative a violazioni, compresi i fondati sospetti, delle normative nazionali e dell'Unione europea che danneggiano l'interesse pubblico o l'integrità dell'amministrazione pubblica o di enti privati, commesse nell'ambito dell'organizzazione dell'ente con cui il Segnalante o denunciante intrattiene uno dei rapporti giuridici considerati dal legislatore (art. 2, comma 1, lett. a, del d.lgs. citato). Le informazioni relative alle violazioni devono riguardare comportamenti, atti o omissioni di cui il segnalante o il denunciante sia venuto a conoscenza in un contesto lavorativo pubblico o privato. Questo contesto comprende non solo i dipendenti ma anche altri soggetti che abbiano una relazione qualificata con la SIM, come consulenti, azionisti, tirocinanti e persone con funzioni di amministrazione, direzione e controllo (art. 2, comma 1, lett. a, del d.lgs. n. 24/2023).

Le informazioni sulle violazioni possono riguardare anche le violazioni non ancora commesse, ma che il *whistleblower* ritiene ragionevolmente possano essere commesse sulla base di elementi concreti (Art. 2, paragrafo 1, lettera b) del d.lgs. n. 24/2023).

Il legislatore ha definito le tipologie di violazioni, di seguito elencate a titolo esemplificativo ma non esaustivo:

Violazioni del diritto nazionale:

- Illeciti civili;
- Illeciti amministrativi;
- Condotte illecite rilevanti ai sensi del d.lgs. n. 231/2001, violazioni dei modelli di organizzazione e gestione previsti dal d.lgs. n. 231/2001;
- Illeciti penali;
- Illeciti contabili;
- Irregolarità di cui all'art. 2, co.1, lett. b) del d.lgs. 24/2023, ovvero "elementi concreti" (indizi sintomatici) tali da far ritenere al segnalante che potrebbe essere commessa una delle violazioni previste dal decreto.



Al fine di agevolare l'identificazione dei fatti che possono essere oggetto di segnalazione, si riporta di seguito un elenco a titolo meramente esemplificativo e non esaustivo di comportamenti rilevanti:

- Violazioni dei codici di comportamento;
- Irregolarità contabili, amministrative e negli adempimenti contabili e fiscali o nella formazione del bilancio d'esercizio;
- False dichiarazioni e false certificazioni;
- Violazioni di norme in materia ambientale, di sicurezza sul lavoro e di controlli;
- Assunzioni non trasparenti;
- Comportamenti volti ad ostacolare le attività di controllo delle Autorità di Vigilanza (ad esempio, omessa consegna di documentazione, presentazione di informazioni false o fuorvianti);
- Promessa o erogazione di denaro, beni o servizi o altri benefici volti a corrompere fornitori, clienti o pubblici ufficiali;
- Azioni suscettibili di danneggiare l'immagine della SIM.

Violazioni del diritto dell'UE:

- Illeciti commessi in violazione della normativa dell'UE;
- Atti od omissioni che ledono gli interessi finanziari dell'UE;
- Atti od omissioni che riguardano il mercato interno e che compromettono la libera circolazione di merci, persone, servizi e capitali;
- Atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'UE.

Segnalazioni non comprese nella procedura:

Sono escluse dal perimetro di applicazione della Procedura le segnalazioni relative a:

- Contestazioni, rivendicazioni o richieste legate a interessi personali del Segnalante, che attengono esclusivamente alla disciplina del rapporto di lavoro o ai rapporti con le figure gerarchicamente sovraordinate, salvo che siano collegate o riferibili a violazioni di norme o regole/procedure interne;
- Violazioni in materia di sicurezza nazionale o appalti relativi a difesa o sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato dell'Unione Europea;
- Violazioni disciplinate obbligatoriamente da atti dell'Unione Europea o nazionali, come indicato nell'art. 1, co. 2, lett. b) del d.lgs. n. 24/2023 (in materia di servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente);
- Fatti o circostanze che rientrano nell'applicazione di disposizioni nazionali o dell'Unione Europea in materia di informazioni classificate, segreto forense o medico, e di segretezza delle deliberazioni degli organi giurisdizionali, o che rientrano nell'applicazione di disposizioni nazionali in materia di procedura penale, autonomia e indipendenza della magistratura, funzioni e attribuzioni del Consiglio Superiore della Magistratura, difesa nazionale, ordine e sicurezza pubblica, esercizio e tutela del diritto dei lavoratori di consultare i propri rappresentanti o i sindacati, protezione contro condotte o atti illeciti commessi in ragione di tali consultazioni, autonomia delle parti sociali e diritto di stipulare accordi collettivi, nonché repressione delle condotte antisindacali;
- Comunicazioni relative a conflitti di interessi;
- Richieste di esercizio dei diritti in materia di protezione dei dati personali nei confronti di CAMPERIO SIM SpA (c.d. diritti privacy), ai sensi del Regolamento (UE) n. 2016/679 (Regolamento Generale sulla Protezione dei Dati - GDPR) e dei d.lgs. 30 giugno 2003 n. 196



(Codice in materia di protezione dei dati personali) e d.lgs. 10 agosto 2018, n. 101 e successive modifiche e integrazioni. Le segnalazioni rientranti nelle categorie sopra indicate verranno inoltrate alle competenti strutture aziendali dalla Funzione Ricevente, che monitorerà comunque gli esiti per rilevare eventuali debolezze del sistema di controllo interno e di gestione dei rischi o impatti sui processi. Non rientrano tra le informazioni sulle violazioni segnalabili o denunciabili le notizie palesemente prive di fondamento, le informazioni che sono già di dominio pubblico o le informazioni acquisite solo sulla base di indiscrezioni o voci non attendibili.

A titolo di esempio puramente indicativo e non esaustivo, si elencano alcune tipologie di comportamenti e casi che non possono essere segnalati:

- L'invio di segnalazioni con finalità puramente diffamatorie o calunniose o che riguardano esclusivamente la vita privata, senza alcun collegamento diretto o indiretto con l'attività aziendale o professionale del soggetto segnalato;
- L'invio di segnalazioni che riguardano esclusivamente il rapporto individuale di lavoro;
- L'invio di segnalazioni di natura discriminatoria nei confronti del soggetto segnalato o tra colleghi;
- L'invio di segnalazioni effettuate con l'unico scopo di danneggiare il soggetto segnalato;
- L'invio di segnalazioni contenenti lamentele personali o conflitti interpersonali. Si specifica che nei casi di invio di segnalazioni vietate, la riservatezza dell'identità del segnalante e le altre misure di tutela potrebbero non essere garantite.

Il segnalante deve essere consapevole che:

- (i) La segnalazione non offre alcuna protezione al segnalante se ha contribuito alla condotta illecita;
- (ii) Resta impregiudicata la responsabilità penale, civile e disciplinare del segnalante in caso di segnalazione calunniosa o diffamatoria, segnalazione effettuata con dolo o colpa grave, o segnalazione effettuata con l'unico scopo di danneggiare il soggetto segnalato.

II. DESCRIZIONE DEL PROCESSO RELATIVO A SEGNALAZIONI INTERNE

2. Gli elementi e le caratteristiche della Segnalazione

Affinché la segnalazione sia efficace e possa essere adeguatamente gestita dai responsabili, è essenziale che contenga dettagli sufficienti che consentano una chiara comprensione dei fatti. La segnalazione può essere presentata direttamente o con l'assistenza di altri, come facilitatori, all'interno dello stesso contesto lavorativo. I dettagli da includere in una segnalazione sono i seguenti:

- dati identificativi del mittente, che possono essere forniti in forma anonima, ma solo se opportunamente documentati;
- informazioni su quando e dove si sono verificati i fatti oggetto della segnalazione.
- una descrizione dettagliata dei fatti stessi;
- informazioni che permettano di identificare il soggetto a cui attribuire i fatti segnalati. È possibile allegare documenti di supporto alla segnalazione e indicare altri soggetti che potrebbero essere a conoscenza dei fatti.



Inoltre, il Segnalante deve dichiarare la presenza di eventuali conflitti di interessi o il suo coinvolgimento nei fatti e atti segnalati. Queste informazioni sono fondamentali per comprendere appieno la natura dei fatti segnalati e per determinare eventuali responsabilità delle diverse persone coinvolte. Nel caso in cui il Segnalante sia coinvolto nei fatti segnalati, nel rispetto delle leggi e regolamenti applicabili, potrà ricevere un trattamento preferenziale rispetto agli altri soggetti coinvolti, salvo casi di dolo o colpa grave. La necessità per la SIM di conoscere l'identità del Segnalante è legata alla possibilità di contattarlo per eventuali chiarimenti o informazioni aggiuntive relative ai fatti segnalati, garantendo sempre la riservatezza e la protezione dell'identità del Segnalante.

2.1 La trasmissione della Segnalazione

I Destinatari della presente Procedura, che vengono a conoscenza di informazioni su violazioni, sono tenuti a effettuare una Segnalazione attraverso i canali interni come di seguito descritti:

- piattaforma di whistleblowing: rappresenta il canale interno di segnalazione raccomandato. La SIM si avvale del supporto di un'applicazione sviluppata su GlobalLeaks, un software libero e open source anche utilizzato dall'ANAC per il proprio sistema di segnalazione. La piattaforma web ("piattaforma *Whistleblowing*") accessibile tramite il link: [camperiosim \(globaleaks.org\)](http://camperiosim.globaleaks.org), consente di effettuare segnalazioni sia in forma scritta che in forma orale tramite un sistema di messaggistica vocale registrata, garantendo la riservatezza dei dati e delle informazioni scambiate tra il segnalante e il gestore del sistema di segnalazione.
- segnalazione in forma scritta da inviare in una busta chiusa per garantire la riservatezza, separando in un'ulteriore busta chiusa riservata, dati identificativi del Segnalante dalla segnalazione stessa. La busta contenente i dati identificativi potrebbe essere facoltativa se il Segnalante desidera rimanere anonimo. Entrambe le buste devono essere poi inserite in una terza busta chiusa, con la dicitura "RISERVATA - all'attenzione della Funzione Ricevente", inoltre, deve riportare l'indirizzo della sede sociale di CAMPERIO SIM S.p.A n°9 – Milano (20121) – Italy;
- segnalazione verbale durante un incontro diretto con la Funzione Ricevente, con registrazione mediante compilazione del verbale contenente le informazioni di cui nell'allegato 1), previa autorizzazione del Segnalante. Il Segnalante deve verificare, correggere o confermare il verbale con la propria firma e data di apposizione. La firma del verbale da parte del Segnalante conferma la ricezione della segnalazione, e una ricevuta viene rilasciata a tal fine.

2.1 Soggetto destinatario della Segnalazione

Indipendentemente dalla modalità di presentazione, tutte le segnalazioni rilevanti vengono ricevute e gestite dalla Funzione Ricevente. Nel caso in cui il Segnalante ritenga che la Funzione Ricevente possa essere in conflitto di interessi rispetto a una specifica Segnalazione, può presentare la Segnalazione direttamente al Presidente del Consiglio di Amministrazione ("**Presidente**"), seguendo la procedura descritta per la segnalazione in forma scritta. La segnalazione viene quindi protocollata e archiviata in modo riservato dalla Funzione Ricevente.

2.2 La registrazione della Segnalazione

Tutte le Segnalazioni, indipendentemente dalla modalità di ricezione, devono vengono registrate entro sette giorni dalla loro ricezione. Nel caso di segnalazione tramite Piattaforma Whistleblowing, la



Funzione Ricevente rilascia un numero di protocollo univoco entro sette giorni dalla ricezione o dalla sottoscrizione del verbale.

2.3 Fase di Istruttoria

Dopo aver ricevuto una Segnalazione, la Funzione Ricevente avvia l'istruttoria nei termini descritti al paragrafo 2.3. L'istruttoria è condotta in modo imparziale e mira a verificare la fondatezza della Segnalazione. Può includere audizioni di persone coinvolte o acquisizione di ulteriori informazioni, a seconda della complessità della Segnalazione, dando priorità alle Segnalazioni ben documentate. Al termine dell'analisi preliminare, la Funzione Ricevente classifica la segnalazione in una delle seguenti categorie:

- a) segnalazione non rilevante: quando la segnalazione non rientra nell'ambito della procedura e viene archiviata, con riscontro al Segnalante se disponibili dati di contatto;
- b) segnalazione pertinente ma non trattabile: quando la segnalazione rientra nell'ambito della procedura ma manca di informazioni sufficienti per avviare ulteriori indagini, viene archiviata, con riscontro al Segnalante se disponibili dati di contatto.
- c) segnalazione esclusa: quando la segnalazione rientra nei casi descritti precedentemente (cfr. paragrafo 5- Sezione I), viene archiviata, con riscontro al Segnalante se disponibili dati di contatto. In caso di segnalazioni calunniose, diffamatorie o effettuate con dolo o colpa grave, la Funzione Ricevente può valutare l'inoltro della segnalazione vietata al Consiglio di Amministrazione, per un possibile procedimento disciplinare.
- d) segnalazione rilevante: quando la segnalazione rientra nell'ambito della procedura e contiene informazioni sufficienti, la Funzione Ricevente la trasmette al Presidente per avviare la fase di verifica, come descritto nel paragrafo successivo.

Una volta completata l'istruttoria, la Funzione Ricevente elabora una relazione finale che riporta le conclusioni raggiunte. Sulla base di tali conclusioni, il Consiglio di Amministrazione può decidere di intraprendere ulteriori azioni correttive, come un'indagine interna dettagliata o l'adozione di misure disciplinari nei confronti delle persone coinvolte, se necessario.

2.4 Fase di gestione della segnalazione

L'organo responsabile della gestione delle segnalazioni è il Consiglio di Amministrazione, che può richiedere il coinvolgimento di professionisti quando necessario. Nel dettaglio, ricevuta la Segnalazione, il Consiglio di Amministrazione, su base documentale e anche in considerazione degli esiti delle preliminari analisi svolte da Funzione Ricevente, dispone l'avvio della successiva fase di istruttoria, ovvero procede all'immediata archiviazione delle Segnalazioni ove riscontri in disaccordo con la valutazione preliminare del Funzione Ricevente che si tratti di Segnalazioni, in quanto:

- i) generiche o non adeguatamente circostanziate;
- ii) palesemente infondate;
- iii) riferite a fatti e/o circostanze oggetto in passato di specifiche attività istruttorie già concluse, ove dalle preliminari verifiche svolte non emergano nuove informazioni tali da rendere necessari ulteriori approfondimenti;
- iv) "circostanziate verificabili", per le quali, alla luce degli esiti delle preliminari verifiche svolte, non emergono elementi tali da supportare l'avvio della successiva fase di istruttoria;



- v) “circostanziate non verificabili”, per le quali, alla luce degli esiti delle preliminari verifiche svolte, non risulta possibile, sulla base degli strumenti di analisi a disposizione, svolgere ulteriori approfondimenti per verificare la fondatezza della Segnalazione.

In presenza di una segnalazione rilevante, il Consiglio di Amministrazione è responsabile di:

- dare un seguito appropriato alle segnalazioni ricevute, fornendo una valutazione sulla loro ammissibilità e garantendo tempi ragionevoli e riservatezza;
- mantenere un canale di comunicazione aperto con il Segnalante;
- fornire una risposta al Segnalante entro tre mesi dalla data di ricezione della segnalazione o, in mancanza di un avviso di ricevimento, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione. Questo viene fatto attraverso la piattaforma o altri mezzi idonei, utilizzando i contatti forniti dal Segnalante, per informarlo sugli sviluppi o sulle misure che verranno prese in relazione alla segnalazione.

Il Consiglio di Amministrazione può richiedere chiarimenti o integrazioni al Segnalante o acquisire informazioni dalle persone coinvolte se ritiene che siano necessarie per la gestione della segnalazione. La riservatezza sull'identità del Segnalante e delle altre persone coinvolte viene mantenuta durante questo processo. Nel caso in cui la valutazione di merito si concluda con l'accertamento delle violazioni oggetto della Segnalazione, il Consiglio di Amministrazione, sentito il parere del Collegio Sindacale, valuta l'eventuale adozione dei provvedimenti, anche disciplinari, di propria competenza. Il Consiglio di Amministrazione può adottare provvedimenti di natura organizzativa e gestionale volti a prevenire il futuro ripetersi della violazione. Al riguardo, il Consiglio di Amministrazione e il Collegio Sindacale possono altresì valutare di segnalare alla Autorità di Vigilanza ovvero alle competenti autorità giudiziarie i fatti oggetto della Segnalazione qualora costituiscano gravi violazioni di disposizioni normative vigenti.

III. PROTEZIONE, SANZIONI, CANALI DI SEGNALAZIONE, TRATTAMENTO DATI

3. Misure di protezione

È vietata ogni forma di ritorsione nei confronti del Segnalante, intendendo per ritorsione ogni comportamento, azione o omissione, anche solo tentati o minacciati, che possa causare al Segnalante un danno ingiusto in diretta o indiretta conseguenza della Segnalazione interna o esterna, della Divulgazione pubblica o della denuncia.

A titolo esemplificativo, alcune delle azioni considerate ritorsioni sono elencate nel decreto come segue:

- i. licenziamento, sospensione o misure equiparate;
- ii. retrocessione di grado o mancata promozione;
- iii. cambio di incarico, trasferimento forzato, riduzione del salario, modifica dell'orario di lavoro;
- iv. sospensione dall'accesso alla formazione o restrizioni all'accesso alla stessa;
- v. emissione di note di demerito o riferimenti negativi;
- vi. adozione di misure disciplinari o altre sanzioni, anche pecuniarie;



- vii. coercizione, intimidazione, molestie o ostracismo;
- viii. discriminazione o qualsiasi forma di trattamento sfavorevole;
- ix. mancata conversione di un contratto a termine in un contratto a tempo indeterminato quando esiste una legittima aspettativa di tale conversione;
- x. mancato rinnovo o risoluzione anticipata di un contratto a termine;
- xi. danneggiamento della reputazione personale, soprattutto sui social media, o danni economici e finanziari, comprese perdite di opportunità e redditi;
- xii. inclusione in elenchi inappropriati, basata su accordi formali o informali settoriali o industriali, che potrebbero impedire al Segnalante di trovare occupazione nel settore o nell'industria in futuro;
- xiii. risoluzione anticipata o annullamento di contratti di fornitura di beni o servizi;
- xiv. annullamento di licenze o permessi;
- xv. richiesta di sottoporsi a esami psichiatrici o medici.

La protezione si estende anche ai Segnalanti anonimi che ritengono di essere stati oggetto di ritorsioni e sono stati successivamente identificati. Le misure di protezione sono applicate conformemente alle disposizioni del capo III del decreto legislativo n. 24/2023 e sono estese alle seguenti categorie:

- categorie di Segnalanti che non rientrano nell'ambito di applicazione oggettivo e/o soggettivo previsto dal decreto legislativo n. 24/2023;
- facilitatori, persone legate al Segnalante da vincoli affettivi o di parentela entro il quarto grado e colleghi di lavoro che lavorano nello stesso contesto e hanno rapporti abituali con il Segnalante;
- enti di proprietà del Segnalante o per i quali lavora, nonché enti operanti nello stesso contesto lavorativo del Segnalante
- chiunque ritenga di aver subito ritorsioni a causa di una Segnalazione può segnalarlo all'Autorità Nazionale Anticorruzione (ANAC).

3.1 Sistema sanzionatorio

Qualsiasi violazione delle disposizioni precedentemente citate potrebbe dar luogo a un procedimento sanzionatorio. In particolare, possono essere soggetti a sanzioni:

- i. il *whistleblower* che ha presentato una segnalazione infondata con dolo o colpa grave;
- ii. chiunque abbia violato la riservatezza del segnalante o commesso atti di "ritorsione";

Nel caso in cui la valutazione si sia conclusa con il mancato accertamento delle violazioni oggetto della Segnalazione, il Segnalante non è soggetto ad alcuna azione disciplinare fatto salvo qualora abbia agito con dolo e/o colpa grave, ovvero la Segnalazione sia stata effettuata al solo scopo di danneggiare o recare pregiudizio al Segnalato. Resta ferma l'eventuale responsabilità nelle ipotesi in cui sia configurabile in capo al Segnalante una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del Codice Penale o ai sensi dell'articolo 2043 del Codice Civile. In ogni caso, ad esito della valutazione di merito della Segnalazione, il Segnalante e il Segnalato sono informati circa la conclusione del processo di valutazione, l'esito della stessa e le relative motivazioni.

3.2 Segnalazione di violazioni alla Banca d'Italia e alla Consob



In conformità all'articolo 4-duodecies del TUF, il personale della SIM ha la facoltà di inviare comunicazioni dirette alle Autorità di Vigilanza, seguendo le procedure operative da queste ultime stabilite (“**Comunicazioni Esterne**”). A tale scopo, Banca d'Italia e Consob:

- i. ricevono, ciascuna per le materie di loro competenza, comunicazioni da parte del personale che segnalano violazioni delle norme del TUF e atti dell'Unione europea direttamente applicabili alle stesse materie;
- ii. possono stabilire condizioni, limiti e procedure per ricevere le comunicazioni, rispettando la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, garantendo al contempo la protezione del segnalante da eventuali rappresaglie, discriminazioni o comportamenti scorretti conseguenti alla comunicazione;
- iii. utilizzano le informazioni contenute nelle comunicazioni, se ritenute rilevanti, esclusivamente per svolgere le loro funzioni di vigilanza;
- iv. coordinano le attività di loro competenza, compresa l'applicazione delle relative sanzioni, attraverso un protocollo d'intesa.

Si precisa che una volta definite le regole relative alle indagini o ai procedimenti avviati dall'autorità giudiziaria in relazione alle questioni segnalate, l'identità del segnalante non è soggetta all'applicazione dell'articolo 15, comma 1, lettera g) del GDPR, e non può essere divulgata durante tutte le fasi della procedura, a meno che il segnalante non dia il suo consenso o che la divulgazione sia indispensabile per la difesa del segnalato. In particolare, per quanto riguarda Consob, le modalità per inviare direttamente comunicazioni riguardanti presunte violazioni delle norme del TUF e atti dell'Unione europea direttamente applicabili sono indicate sul sito web dell'Autorità (<http://www.consob.it/web/area-pubblica/whistleblowing>). Vengono fornite tutte le protezioni previste dalla Legge 30 novembre 2017, n. 179, per gli autori di comunicazioni relative a reati o irregolarità di cui sono a conoscenza in ambito lavorativo, compresa la nullità di possibili provvedimenti disciplinari con finalità punitive o discriminatorie nei confronti del segnalante.

Le comunicazioni a Banca d'Italia da parte del personale degli intermediari vigilati sono effettuate tramite l'apposito modulo e possono essere inviate tramite la piattaforma “Servizi online”, selezionando l'opzione “Invia una comunicazione” sul sito web dell'Autorità (<https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/index.html>), oppure per posta ordinaria all'indirizzo della Banca d'Italia – Servizio CRE – divisione SRE – a Roma, Via Nazionale n. 91, con la dicitura "riservato" sulla busta. La Banca d'Italia si riserva il diritto, se lo ritiene opportuno, di contattare il segnalante per ulteriori informazioni o chiarimenti, nel rispetto del segreto d'ufficio che copre tutti i dati e le informazioni ottenuti nell'ambito delle attività di vigilanza. La Banca d'Italia garantisce la riservatezza dei dati personali del segnalante, al fine di tutelare quest'ultimo da possibili ritorsioni.

3.3 Divulgazione pubblica

Il Decreto Legislativo n. 24/2023, all'articolo 15, prevede una modalità aggiuntiva di segnalazione denominata “divulgazione pubblica”. Con la divulgazione pubblica, le informazioni relative alle violazioni vengono rese di dominio pubblico attraverso la stampa, mezzi elettronici o altri mezzi di

3.4 Formazione del personale

Al fine di promuovere l'uso dei sistemi interni di comunicazione e diffondere una cultura della legalità, la SIM si impegna a fornire al personale informazioni chiare, precise e complete sulle disposizioni della presente Procedura. In particolare, si fornisce dettagli sul procedimento di comunicazione interno e sulle



misure atte a proteggere la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione. Il personale è informato che l'articolo 15, comma 1, lettera g) del GDPR, che garantisce il diritto del presunto responsabile di conoscere l'origine dei dati personali, non si applica all'identità del segnalante, la cui divulgazione è consentita solo con il suo consenso o quando è indispensabile per la difesa del segnalato.

3.5 Trattamento dei dati personali e conservazioni della documentazione

Ogni trattamento dei dati personali, incluso quello effettuato attraverso la Piattaforma, è eseguito nel pieno rispetto degli obblighi di riservatezza stabiliti dall'articolo 12 del Decreto Legislativo n. 24/2023 e in conformità con la normativa sulla protezione dei dati personali, come definito nel Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati - GDPR), nel Decreto Legislativo 30 giugno 2003 n. 196 e nel Decreto Legislativo 18 maggio 2018 n. 51.

La protezione dei dati personali è garantita non solo per il *whistleblower* (nelle segnalazioni non anonime) ma anche per il Facilitatore e per la persona coinvolta o menzionata nella segnalazione.

Tutti gli interessati ricevono informazioni dettagliate sul trattamento dei loro dati personali tramite la pubblicazione sulla Piattaforma *Whistleblowing* e sul sito web aziendale.

In ottemperanza all'articolo 13, comma 6, del Decreto Legislativo n. 24/2023, è stata condotta una valutazione dell'impatto sulla protezione dei dati (Data Privacy Impact Assessment - DPIA) conformemente all'articolo 35 del Regolamento GDPR. Questo processo mira a definire le misure tecniche e organizzative necessarie per ridurre il rischio per i diritti degli interessati, inclusa la messa in atto di adeguate misure di sicurezza per prevenire trattamenti non autorizzati o illeciti.

Al fine di garantire la gestione e la tracciabilità delle segnalazioni e delle attività correlate, la Funzione Ricevente si occupa di mantenere aggiornate tutte le informazioni relative alle segnalazioni e garantisce, attraverso l'uso della Piattaforma, la conservazione di tutta la documentazione correlata per il periodo strettamente necessario a definire le segnalazioni, e comunque per non più di 5 anni a partire dalla data di conclusione dell'attività istruttoria condotta dal Consiglio di Amministrazione. I dati personali che chiaramente non sono pertinenti al trattamento di una specifica segnalazione non vengono raccolti o, se raccolti per errore, vengono eliminati tempestivamente. Gli originali delle segnalazioni pervenute in formato cartaceo sono conservati in un apposito ambiente protetto.



ALLEGATO 1

VERBALE PER LA SEGNALAZIONE INTERNA DELLE VIOLAZIONI

Nome e cognome del Segnalante

.....

Inquadramento e qualifica professionale

.....

Sede di lavoro

.....

Recapiti (n. telefono/e-mail)

.....

Luogo in cui si è verificato il fatto Data/periodo in cui si è verificato il fatto

.....

Descrizione dei fatti oggetto di Segnalazione

.....

.....

Ambito normativo di riferimento (eventuale)

.....

.....

Generalità o altri elementi che consentano di identificare il soggetto o i soggetti che hanno posto in essere i fatti segnalati Soggetti che possono riferire sui fatti oggetto di segnalazione;

.....

.....

Soggetti a conoscenza dei fatti oggetto di Segnalazione (eventuale)

.....



.....
Ulteriori informazioni che possono fornire utile riscontro circa la sussistenza dei fatti oggetto di Segnalazione (eventuale)

.....
.....

Documenti allegati che possono confermare la fondatezza dei fatti (eventuale)

.....
.....

Il sottoscritto dichiara l'assenza di qualsiasi interesse privato collegato alla segnalazione oppure Il sottoscritto dichiara la sussistenza di un interesse privato collegato alla segnalazione, di seguito descritto:

.....
.....

Luogo e data Firma

Segnalante

Funzione Ricevente

(Responsabile Funzione Compliance)