

Policy e disposizioni per la segnalazione di condotte illecite (Whistleblowing)

Predisposta dalla Funzione *Operations*

Rivista dalla Funzione *Compliance*

Versione	Approvata da	Data approvazione	Descrizione sintetica modifiche
1.0	CdA	28/02/2018	
2.0	CdA	08/02/2024	Adeguamenti normativi e organizzativi

INDICE

1. Premessa.....	3
2. Quadro normativo di riferimento.....	3
3. Ruoli e responsabilità.....	4
4. Ambito di applicazione.....	4
5. Soggetti che godono della protezione in caso di segnalazione.....	6
6. Soggetti che godono della protezione diversi da chi segnala.....	7
7. Oggetto della segnalazione.....	7
8. Contenuti esclusi dalla segnalazione.....	7
9. Elementi e caratteristiche delle segnalazioni.....	8
10. Segnalazioni anonime e la loro trattazione.....	8
11. Tutele del Segnalante.....	9
12. trattamento dei dati personali.....	13
13. Trattamento delle segnalazioni diffamatorie.....	14
14. Modalità operative.....	15
15. Responsabile del Sistema di segnalazione interna o Organismo Ricevente.....	15
16. Esame delle Segnalazioni.....	16
17. Chiusura dell'istruttoria ed attuazione delle azioni definite in fase di analisi delle Segnalazioni.....	16
18. Conservazione della documentazione.....	17

1. Premessa

Scopo della presente Policy è quello di definire ed esporre le modalità operative e i flussi di comunicazione da seguire in merito alle segnalazioni di violazioni del diritto dell'Unione e delle normative nazionali (c.d. "whistleblowing"), quali ad esempio illeciti amministrativi, contabili, civili o penali e condotte illecite rilevanti ai sensi del D. lgs. 231/2001 (norme in materia di lotta contro la corruzione – riciclaggio di denaro – controllo interno contabile – finanziamento del terrorismo) alla protezione dei consumatori, alla tutela dei dati personali, alla sicurezza delle reti e dei sistemi informativi, alle violazioni in materia di concorrenza, o che possano riguardare qualsiasi altra circostanza che possa porre in pericolo gli asset fisici e reputazionali di Marzotto SIM (di seguito anche la "SIM" o la "Società").

In considerazione del modello di *business* ed organizzativo adottato dalla SIM, della dimensione contenuta della stessa, della prudente propensione al rischio espressa dal Consiglio di Amministrazione, nonché della natura della clientela, si è ritenuto di introdurre una *policy* – corredata delle istruzioni operative necessarie per assicurare il rispetto dei principi – per tutte le attività di segnalazione interna.

Infatti, come si dirà nel successivo paragrafo, solo alcune delle direttive europee e delle leggi italiane che introducono procedure di segnalazione sono applicabili alla SIM.

La *policy* e le regole operative descritte nei successivi paragrafi si affiancano ai principi già richiamati nel Codice di comportamento e alle altre *policy*/procedure per la segnalazione interna di fattispecie anomale o rischiose (ad esempio: segnalazioni sospette di riciclaggio, segnalazioni di abusi di mercato).

2. Quadro normativo di riferimento

Considerato il modello di *business* ed organizzativo della SIM, nonché avuta presente la clientela *target* dei servizi di investimento, le norme europee e nazionali rilevanti sono rappresentate da:

- decreto legislativo 10 marzo 2023, n. 24 che recepisce la 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. disciplina *whistleblowing*). Per effetto delle disposizioni del Decreto sono abrogati: l'art. 54 bis del Decreto legislativo 30 marzo 2001 n. 165 TUIP per gli enti pubblici; l'art. 6, commi 2 ter e 2 quater, del Decreto 231; l'art. 3 del d. lgs. 179/2017. È stato invece modificato l'art. 6 comma 2 bis del Decreto 231;
- 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;
- Linee Guida ANAC adottate con delibera del 12 luglio 2023;
- Linee Guida Confindustria, "Guida operativa per gli enti privati" di ottobre 2023;
- Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 (c.d. "V Direttiva antiriciclaggio") e art. 48 D. Lgs. n. 90/2017;
- Atto del Senato n. 2208 del 18 ottobre 2017 e decreto-legge "whistleblowing" approvato dalla Camera dei deputati il 15 novembre 2017, ai fini dell'estensione dei presidi adottati nell'ambito del Modello di organizzazione, gestione e controllo di cui

al D. Lgs. n. 231/2001 e s.m.i.;

- Articolo 4-undecies del D. Lgs. 58/1998 e s.m.i. (anche “Testo Unico della Finanza”) relativamente all’adozione di procedure per la segnalazione interna all’azienda e da parte del personale, di atti o fatti che possano costituire violazioni delle norme.

Non rilevano invece gli obblighi di segnalazione interna per le banche di cui all’art. 52-bis del D. Lgs. n. 385/1993 e s.m.i.; le misure di cui all’art. 7 del Codice di autodisciplina della società quotate (Borsa Italiana) nonché le linee guida espresse in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell’art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)”.

3. Ruoli e responsabilità

Consiglio di Amministrazione

Nell’ambito dei compiti di indirizzo strategico ed organizzativo, il Consiglio di Amministrazione è responsabile di:

- a) definire la *Policy* di Whistleblowing (Segnalazione di condotte illecite) e valutarne, con cadenza almeno annuale, l’adeguatezza in relazione alla complessiva attività svolta, alla tolleranza al rischio ed al livello di patrimonializzazione posseduto;
- b) nominare il responsabile del Sistema interno di segnalazione delle violazioni che assicura il corretto svolgimento delle procedure, garantendo adeguati presidi d’indipendenza;
- c) promuovere la cultura della legalità e della trasparenza al fine di incentivare l’uso del meccanismo delle segnalazioni affinché l’intera organizzazione operi in un ambiente favorevole e propizio a incoraggiare le segnalazioni di possibili comportamenti illeciti o irregolari nella consapevolezza che le stesse saranno ricevute, analizzate e verificate con il necessario rigore e nel rispetto della riservatezza e della protezione dei dati personali del segnalante e del segnalato;
- d) richiedere di essere informato in relazione ai casi di segnalazione di violazioni e che gli siano riferite con tempestività le violazioni più significative;
- e) effettuare una valutazione dell’effettivo livello di rischio cui è esposta la Società, qualora la violazione sia stata accertata.

Amministratore Delegato

È responsabile, sulla base delle direttive impartite dall’Organo amministrativo, dell’attuazione, del mantenimento e del monitoraggio della politica di Whistleblowing.

In particolare, l’Alta Direzione:

- a) attua gli obiettivi fissati dall’Organo amministrativo;
- b) definisce e rende note alle unità organizzative interessate le procedure operative interne relative al Whistleblowing;
- c) propone all’Organo amministrativo, anche alla luce delle indicazioni della funzione di *Compliance*, eventuali modifiche alla politica di Whistleblowing;
- d) dà attuazione alle indicazioni dell’organo amministrativo in ordine alle misure da adottare per correggere le anomalie riscontrate e apportare miglioramenti.

4. Ambito di applicazione

Le norme in tema di *whistleblowing* obbligano Marzotto SIM a:

- a) Adottare una procedura per la segnalazione interna da parte del Segnalante

(*whistleblower*) di violazioni potenziali o effettive da parte di un altro soggetto (anche “il Segnalato”) delle seguenti disposizioni:

Violazioni delle disposizioni normative nazionali

In tale categoria rientrano gli illeciti penali, civili, amministrativi o contabili diversi rispetto a quelli specificamente individuati come violazioni del diritto UE:

- Ricettazione, riciclaggio, autoriciclaggio e finanziamento del terrorismo. Si fa riferimento – oltre che nel codice penale agli artt. 648 bis, 648 ter e 648 ter., al Decreto Legislativo 21 novembre 2007, n. 231 (di seguito, il “**Decreto**” o “**D. Lgs. 231/2007**”), come modificato dal D. Lgs. 90/2017 in attuazione della direttiva UE 2015/ 849 (**c.d. “IV Direttiva Antiriciclaggio”**) – concernente la prevenzione dell’uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo - da ultimo modificato dal D.Lgs. 4 ottobre 2019, n. 125, Direttiva UE n. 2018/843 (**c.d. V° Direttiva**), e dalle relative disposizioni di attuazione emanate dal Ministro dell’economia e delle finanze, dall’Unità di Informazione Finanziaria per l’Italia e dalla Banca d’Italia. Nello specifico si richiamano– le violazioni delle regole operative contenute nel Manuale operativo antiriciclaggio, cui per comodità si fa rimando;
- Illeciti civili;
- Illeciti amministrativi;
- Illeciti penali;
- Illeciti contabili;
- Irregolarità - non incluse tra le violazioni del diritto nazionale ma possono costituire “elementi concreti” (indici sintomatici) - di cui all’ art. 2, co. 1, lett. b) d.lgs. 24/2023 - tali da far ritenere al segnalante che potrebbe essere commessa una delle violazioni previste;
- TUF e regolamenti attuativi, ovvero tutte le norme interne che riguardano la prestazione dei servizi di investimento. In tale contesto rientrano altresì le norme aziendali in materia di conflitti di interesse, operazioni personali, gestione degli incentivi, valutazione di adeguatezza del prodotto offerto alla clientela;
- I reati presupposto per l’applicazione del Decreto 231; in tale contesto tutti i presidi posti in essere intesi come “Protocolli di prevenzione dei reati di cui al Modello organizzativo 231/2001 di Marzotto SIM”. A titolo esemplificativo e non esaustivo si fa riferimento ai contenuti del Codice Etico e di Comportamento, ai contenuti della “Parte Speciale” del Modello organizzativo 231/2001 adottato dal Consiglio di Amministrazione; a tutte le disposizioni e procedure aziendali direttamente o indirettamente riconducibili ai reati presupposto ex D.Lgs.231/2001.

Violazioni del diritto dell’UE

- Illeciti commessi in violazione della normativa dell’UE indicata nell’Allegato 1 al d.lgs. n. 24/2023 e di tutte le disposizioni nazionali che ne danno attuazione (anche se queste ultime non sono espressamente elencate nel citato allegato);
- Atti od omissioni che ledono gli interessi finanziari dell’Unione Europea (art. 325 del TFUE lotta contro la frode e le attività illegali che ledono gli interessi finanziari dell’UE) come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell’UE;

- Atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE). Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposta sulle società e i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società (art. 2, co. 1, lett. a) n. 5) Atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea nei settori sopra indicati;
- Riciclaggio e del finanziamento del terrorismo. Si fa riferimento – in particolare - alle violazioni delle regole operative contenute nel Manuale operativo antiriciclaggio, cui per comodità si fa rimando.

Possono essere oggetto di segnalazione anche quegli elementi che riguardano condotte volte ad occultare le violazioni. Si pensi, ad esempio, all'occultamento o alla distruzione di prove circa la commissione della violazione.

- b) Tutelare la riservatezza dei soggetti che decidono di segnalare illeciti, anche al fine di escludere condotte ritorsive da parte del Segnalato, ovvero delle figure dalle quali il Segnalante dipende gerarchicamente. Ciò in particolare nell'ipotesi in cui la segnalazione comprometta una specifica operazione ovvero infici la generazione dei ricavi;
- c) Tutelare i soggetti Segnalati presunti autori della violazione;
- d) Sviluppare uno specifico canale di segnalazione, anonimo e indipendente, proporzionato alla natura e alle dimensioni della SIM.

La mancata adozione di un sistema interno di segnalazione comporta la possibile elevazione di sanzioni a discapito dei membri dell'Organo con funzione di supervisione strategica.

5. Soggetti che godono della protezione in caso di segnalazione

Il novero dei soggetti – genericamente individuati come “il Segnalante” o “il *whistleblower*” – cui è assicurata la massima tutela in caso di segnalazione, denuncia o divulgazione, ai sensi della vigente normativa, sono le seguenti persone che prestano la loro attività lavorativa o intrattengono rapporti con la Società:

- Lavoratori subordinati
- Soggetti terzi che intrattengono rapporti e relazioni d'affari durevoli con la Società (e.g. collaborazioni coordinate e continuative, Lavoratori autonomi consulenti, liberi professionisti che prestano la propria attività presso la SIM.
- Volontari e tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la SIM
- i fornitori di beni e servizi;
- Azionisti.
- persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto presso la SIM.

Le segnalazioni sono ammesse anche:

- quando il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali (ad es. candidati);

- successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite prima dello scioglimento del rapporto stesso (e.g. pensionati).

Tutti i suddetti soggetti, in caso di segnalazione la SIM ne garantisce la tutela non solo se la segnalazione avvenga in costanza del rapporto di lavoro o di altro tipo di rapporto giuridico, ma anche durante il periodo di prova e anteriormente (ad esempio, nella fase precontrattuale) o successivamente allo scioglimento del rapporto giuridico.

6. Soggetti che godono della protezione diversi da chi segnala

La tutela è riconosciuta, oltre ai sopra indicati soggetti che effettuano segnalazioni, anche a quei soggetti che, tuttavia, potrebbero essere destinatari di ritorsioni, intraprese anche indirettamente, in ragione del ruolo assunto nell'ambito del processo di segnalazione e/o del particolare rapporto che li lega al segnalante o denunciante. Tali soggetti possono essere:

- Facilitatore, persona fisica che assiste e supporta il Segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- Persone del medesimo contesto lavorativo del segnalante e che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado;
- Collegli di lavoro del segnalante, che lavorano nel medesimo contesto lavorativo dello stesso e che hanno con detta persona un rapporto abituale e corrente;
- Enti presso i quali il segnalante lavora.

7. Oggetto della segnalazione

Sono oggetto di segnalazione le informazioni sulle violazioni, compresi i fondati sospetti, di normative nazionali e dell'Unione europea che ledono o possono ledere l'interesse della SIM commesse nell'ambito dell'organizzazione con cui il segnalante intrattiene uno dei rapporti giuridici qualificati.

Le informazioni sulle violazioni possono riguardare anche le violazioni non ancora commesse che il *whistleblower*, ragionevolmente, ritiene potrebbero esserlo sulla base di elementi concreti. Tali elementi possono essere anche irregolarità e anomalie (indici sintomatici) che il segnalante ritiene possano dar luogo ad una violazione¹.

Le informazioni sulle violazioni devono essere apprese nel contesto lavorativo del segnalante e devono riguardare comportamenti, atti od omissioni di cui il segnalante sia venuto a conoscenza nel contesto lavorativo.

8. Contenuti esclusi dalla segnalazione

Non sono ricomprese tra le informazioni sulle violazioni segnalabili:

- le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite solo sulla base di indiscrezioni o

¹ Non sono ricomprese tra le informazioni sulle violazioni segnalabili o denunciabili, le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (cd. voci di corridoio).

vociferazioni scarsamente attendibili (cd. voci di corridoio);

- Le contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate;
- Le segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea;
- Le segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea.

9. Elementi e caratteristiche delle segnalazioni

Le Segnalazioni devono essere effettuate in buona fede e non devono essere rivolte a denunciare situazioni di natura esclusivamente personale, fatte salve le molestie a sfondo sessuale, razziale o di genere.

È necessario 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.

È necessario che 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 (indizi) precisi e concordanti² 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. Ove quanto segnalato non sia adeguatamente circostanziato, chi gestisce le segnalazioni può chiedere elementi integrativi al segnalante tramite il canale a ciò dedicato o anche di persona, ove il segnalante abbia richiesto un incontro diretto.

10. Segnalazioni anonime e la loro trattazione

La SIM considera le segnalazioni anonime ricevute attraverso i canali interni alla stregua di segnalazioni ordinarie.

Le segnalazioni "anonime", effettuate senza identificazione del *whistleblower*, vengono prese in considerazione purché anch'esse adeguatamente circostanziate e rese con dovizia di particolari, ove cioè siano in grado di far emergere fatti e situazioni relazionandoli a contesti determinati. Sono considerate anonime le segnalazioni che sono trasmesse a mezzo della piattaforma informatica utilizzando la modalità "Invia segnalazione anonima". In questo caso il *whistleblower* "anonimo", ha comunque la facoltà di interagire con l'istruttore della piattaforma mediante scambio di messaggi ed eventuali documenti.

² Un indizio è da considerarsi "preciso" quando non è suscettibile di diverse interpretazioni mentre è "concordante" nel senso che ci debbano essere più indizi che confluiscono nella medesima direzione.

11. Tutele del Segnalante

Tutte le segnalazioni sono trattate e classificate con il livello massimo di riservatezza ed è garantita in ogni caso la riservatezza e la protezione dei dati personali del soggetto Segnalante e del soggetto eventualmente Segnalato.

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

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

Il Segnalante in buona fede è garantito e tutelato contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, a prescindere dai soggetti coinvolti. Il segnalante, infatti, non subisce condotte ritorsive o discriminatorie o comunque sleali per aver effettuato la segnalazione. Qualsiasi forma di ritorsione, anche vessatoria, è vietata e pertanto sarà passibile di provvedimento disciplinare.

Le misure di protezione si applicano anche ai facilitatori ed altri soggetti in stretto legame (di tipo familiare e/o lavorativo) con il segnalante secondo quanto previsto dal D.lgs. n. 24/2023.

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

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

La protezione dalle ritorsioni è estesa anche al Segnalante che ha effettuato una divulgazione pubblica.

1. Tutela della riservatezza del Segnalante

La SIM deve garantire la riservatezza dell'identità del Segnalante, ciò anche al fine di evitare l'esposizione dello stesso a misure ritorsive che potrebbero essere adottate a seguito della segnalazione.

L'identità della persona Segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate senza il consenso espresso della stessa persona Segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

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.

In tali casi, è dato preventivo avviso alla persona Segnalante mediante comunicazione scritta delle ragioni che rendono necessaria la rivelazione dei dati riservati.

Qualora il soggetto Segnalante neghi il proprio consenso, la segnalazione non potrà essere

utilizzata nel procedimento disciplinare che, quindi, non potrà essere avviato o proseguito in assenza di elementi ulteriori sui quali fondare la contestazione.

La riservatezza, oltre che all'identità del Segnalante, viene garantita anche a qualsiasi altra informazione o elemento della segnalazione dal cui disvelamento si possa dedurre direttamente o indirettamente l'identità del Segnalante. La riservatezza viene garantita anche nel caso di segnalazioni effettuate in forma orale attraverso linee telefoniche o, in alternativa, sistemi di messaggistica vocale ovvero, su richiesta della persona Segnalante, mediante un incontro diretto con chi tratta la segnalazione.

La violazione della riservatezza in ordine all'identità del Segnalante costituisce illecito disciplinare ai sensi del Sistema Sanzionatorio di cui al Modello Organizzativo 231/01.

Si tutela la riservatezza del Segnalante anche quando la segnalazione perviene a personale diverso da quello autorizzato e competente a gestire le segnalazioni, al quale, comunque, le stesse vanno trasmesse senza ritardo entro massimo 7 (sette) giorni. Per rivelare l'identità del Segnalante, oltre al consenso espresso dello stesso, si richiede anche una comunicazione scritta delle ragioni di tale rivelazione:

- nel procedimento disciplinare laddove il disvelamento dell'identità del Segnalante sia indispensabile per la difesa del soggetto a cui viene contestato l'addebito disciplinare;
- nei procedimenti instaurati in seguito a segnalazioni interne laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta.

2. Tutela da eventuali ritorsioni

A tutela del *whistleblower* è previsto 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 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”*. Può consistere sia in atti o provvedimenti che in comportamenti od omissioni che si verificano nel contesto lavorativo e che arrecano pregiudizio ai soggetti tutelati. La ritorsione può essere anche *“solo tentata o minacciata”*.

Elencazione delle ritorsioni con carattere non esaustivo:

- licenziamento, sospensione o misure equivalenti;
- retrocessione di grado o mancata promozione;
- mutamento di funzioni, cambiamento del luogo di lavoro, riduzione dello stipendio, modifica dell'orario di lavoro;
- sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- note di demerito o referenze negative;
- adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- coercizione, intimidazione, molestie o ostracismo;
- discriminazione o comunque trattamento sfavorevole;
- 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;

- mancato rinnovo o risoluzione anticipata di un contratto di lavoro a termine;
- danni, anche alla reputazione della persona, in particolare sui social media, o pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- 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;
- conclusione anticipata o annullamento del contratto di fornitura di beni o servizi;
- annullamento di una licenza o di un permesso;
- richiesta di sottoposizione ad accertamenti psichiatrici o medici.

L'applicazione del regime di protezione contro le ritorsioni è subordinata ad alcune condizioni e requisiti:

- a. Il soggetto ha segnalato in base ad una convinzione ragionevole che le informazioni sulle violazioni segnalate siano veritiere e rientranti nell'ambito oggettivo di applicazione del decreto.
- b. La segnalazione è stata effettuata nel rispetto della disciplina prevista dal d.lgs. 24/2023.
- c. È necessario un rapporto di consequenzialità tra segnalazione effettuata e misure ritorsive subite.
- d. Non sono sufficienti invece i meri sospetti o le "voci di corridoio". Non rilevano la certezza dei fatti né i motivi personali che hanno indotto il soggetto a segnalare.

In difetto di tali condizioni:

- le segnalazioni non rientrano nell'ambito della disciplina di *whistleblowing* e quindi la tutela prevista non si applica a chi segnala;
- analogamente si esclude la protezione riconosciuta ai soggetti diversi, che in ragione del ruolo assunto nell'ambito del processo di segnalazione/denuncia e/o del particolare rapporto che li lega al segnalante o denunciante, subiscono indirettamente ritorsioni.

La protezione prevista in caso di ritorsioni non trova applicazione in caso di accertamento con sentenza, anche non definitiva di primo grado nei confronti del Segnalante, della responsabilità penale per i reati di calunnia o diffamazione o comunque per i medesimi reati commessi con la denuncia, ovvero della responsabilità civile, per aver riferito informazioni false riportate intenzionalmente con dolo o colpa. Nei casi di accertamento delle dette responsabilità, al soggetto Segnalante e denunciante è inoltre applicata una sanzione disciplinare. La SIM ha inserito anche nel MOG 231 questa specifica fattispecie sanzionabile.

3. Le limitazioni della responsabilità per chi segnala

All'insieme delle tutele riconosciute dalla disciplina al Segnalante si devono ascrivere anche le limitazioni della responsabilità rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni. Si tratta di limitazioni che operano al ricorrere di determinate condizioni in assenza delle quali vi sarebbero conseguenze in termini di responsabilità penale, civile, amministrativa.

Reati non configurabili nei casi di diffusione di informazioni coperte dall'obbligo di segreto se opera la discriminante, in particolare rispetto a:

- Rivelazione e utilizzazione del segreto d'ufficio (art. 326 c.p.);
- Rivelazione del segreto professionale (art. 622 c.p.); Rivelazione dei segreti scientifici e industriali (art. 623 c.p.);
- Violazione del dovere di fedeltà e di lealtà (art. 2105 c.c.);
- Violazione delle disposizioni relative alla tutela del diritto d'autore;
- Violazione delle disposizioni relative alla protezione dei dati personali Rivelazione o diffusione di informazioni sulle violazioni che offendono la reputazione della persona coinvolta

Devono ricorrere cumulativamente due condizioni perché l'esclusione della responsabilità operi nei casi di diffusione di informazioni:

- 1) Fondati motivi, al momento della rilevazione o diffusione delle informazioni, per ritenere che tale rivelazione o diffusione è necessaria per svelare la violazione.
- 2) Effettuare la segnalazione nel rispetto delle condizioni che il legislatore ha previsto nel d.lgs. n. 24/2023 per beneficiare delle tutele.
- 3) Esclusione di responsabilità in caso di accesso lecito alle informazioni segnalate o ai documenti contenenti dette informazioni.
- 4) Esclusione della responsabilità penale e ogni altra responsabilità, anche di natura civile o amministrativa, anche per i comportamenti, gli atti o le omissioni se collegati alla segnalazione e strettamente necessari a rivelare la violazione.

Tutela della riservatezza del Segnalato

La riservatezza della persona coinvolta e della persona menzionata viene garantita anche:

- nel caso di segnalazioni effettuate in forma orale attraverso linee telefoniche o, in alternativa, sistemi di messaggistica vocale ovvero, su richiesta della persona Segnalante, mediante un incontro diretto fissato entro un termine ragionevole;
- quando la segnalazione perviene a personale diverso da quello autorizzato al trattamento delle segnalazioni, al quale va in ogni caso trasmessa senza ritardo. La persona Segnalata può essere sentita o viene sentita, dietro sua richiesta, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti. Tale soggetto non ha il diritto di essere sempre informato della segnalazione che lo riguarda ma solo nell'ambito del procedimento eventualmente avviato nei suoi confronti a seguito della conclusione della gestione della segnalazione e nel caso in cui tale procedimento sia fondato in tutto o in parte sulla segnalazione.

La presente procedura lascia impregiudicata la responsabilità penale e disciplinare del Segnalante/dipendente nell'ipotesi di Segnalazioni calunniose o diffamatorie ai sensi del codice penale e dell'art. 2043 del Codice civile.

Sono, altresì, fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente procedura, quali segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il Segnalato o altri soggetti e comunque ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione di

quanto previsto e oggetto della presente procedura.

12. trattamento dei dati personali

Al fine di garantire il diritto alla protezione dei dati personali alle persone segnalanti è previsto che l'acquisizione e gestione delle segnalazioni avvenga in conformità alla normativa in tema di tutela dei dati personali³.

La tutela dei dati personali va assicurata non solo alla persona Segnalante ma anche agli altri soggetti cui si applica la tutela della riservatezza, quali il facilitatore, la persona coinvolta e la persona menzionata nella segnalazione in quanto "interessati" dal trattamento dei dati.

Si riportano di seguito le qualifiche dei soggetti che trattano i dati personali:

- Titolare del trattamento: Marzotto SIM
- Responsabili del trattamento – Soggetti gestori delle segnalazioni – Amministratore Indipendente e Responsabile Compliance
- Persone autorizzate - Persone espressamente designate dal titolare del trattamento che gestiscono e trattano le segnalazioni

I titolari del trattamento, i responsabili del trattamento e le persone autorizzate a trattare i dati personali sono tenuti a rispettare alcuni principi fondamentali:

- Trattare i dati in modo lecito, corretto e trasparente;
- Raccogliere i dati al solo fine di gestire e dare seguito alle segnalazioni;
- Garantire che i dati siano adeguati, pertinenti e limitati a quanto necessario per le finalità per le quali sono trattati;
- Assicurare che i dati siano esatti e aggiornati;
- Conservare i dati per il tempo necessario al trattamento della specifica segnalazione. Non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione;
- Assicurare il trattamento in maniera da garantire la sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, distruzione e dal danno accidentali;
- Rispettare il principio della *privacy by design* e della *privacy by default*;
- Effettuare la valutazione d'impatto sulla protezione dei dati;
- Rendere *ex-ante* ai possibili interessati un'informativa sul trattamento dei dati personali mediante la pubblicazione di documenti informativi (ad esempio sul sito

³ In particolare, al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (GDPR), al d.lgs. n. 196 del 30 giugno 2003, adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101. e al d.lgs. 51/2018 recante "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio".

web);

- Assicurare l'aggiornamento del registro delle attività di trattamento;
- Garantire il divieto di tracciamento dei canali di segnalazione;
- Garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante.

La responsabilità in caso di violazione della disciplina sulla tutela dei dati personali ricade in capo al titolare del trattamento laddove tale violazione sia commessa dalle persone autorizzate o dai responsabili del trattamento.

La responsabilità ricade in capo al responsabile del trattamento nel caso in cui la suddetta violazione è commessa da persone autorizzate da quest'ultimo. In tali casi, il Garante per la protezione dei dati personali può adottare provvedimenti correttivi e, nei casi previsti dalla legge, applicare sanzioni amministrative pecuniarie. Tali sanzioni amministrative non si applicano in relazione ai trattamenti svolti in ambito giudiziario. Le medesime violazioni possono inoltre rilevare sotto il profilo penale e dar luogo a responsabilità civile. La persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione non possono esercitare – per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata - i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento³²). Dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante. In tali casi, dunque, al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della protezione dei dati personali.

13. Trattamento delle segnalazioni diffamatorie

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

Il Segnalante deve comunque ottemperare ai principi di correttezza del Codice di Comportamento adottato da Marzotto SIM, è responsabile dell'eventuale reato di calunnia o diffamazione perpetrato mediante l'infondata e/o pretestuosa segnalazione di un dipendente o collaboratore.

Parimenti, il Segnalante è a conoscenza del fatto che l'assolvimento di attività in tema di *whistleblowing* non si sostituisce ad altri obblighi di segnalazione che ricadono sui dipendenti e collaboratori della SIM. In particolare, la segnalazione *whistleblowing* su errati comportamenti delle società o di singoli dipendenti o collaboratori in tema di contrasto al riciclaggio o finanziamento al terrorismo, non si sostituisce all'obbligo di inviare una segnalazione di operazione sospetta di riciclaggio o di finanziamento del terrorismo al Delegato SOS.

14. Modalità operative

Il Consiglio di Amministrazione della SIM ha scelto di adottare quale procedura per la segnalazione interna delle possibili violazioni l'attivazione dei seguenti canali:

- Piattaforma on-line, basata su una infrastruttura esterna, per una fruizione anonima, senza tracciatura dei dati tecnici relativi alla rete ed al dispositivo utilizzato, garantendo così il massimo della riservatezza. L'accesso alla piattaforma on-line dovrà avvenire mediante *click* al seguente *link*: <https://marzottosim.openblow.it/>, pubblicato anche sul sito istituzionale della SIM www.marzottosim.com.
Per meglio comprendere le modalità di utilizzo della Piattaforma si riporta il link per accedere al manuale (<https://docs.laserromae.it/docs/openblow/usermanual>)
- canale orale mediante l'invio della segnalazione chiamando il seguente numero di telefono: 390282900013. Al termine della chiamata verrà rilasciata una key che dovrà essere segnata dal Segnalante e inserita nella Piattaforma *on-line* per eventualmente proseguire l'interlocuzione con l'istruttore;
- richiesta inoltrata mediante la Piattaforma di incontro diretto con il Responsabile della Segnalazione;
- mail inviata all'indirizzo dell'OdV odv@marzottosim.com con reindirizzo a pino.ruscio@lprconsulting.it;
- in forma cartacea a mezzo posta ordinaria con la dicitura "riservata" all'indirizzo dell'OdV LPR Management Consulting S.r.l. Residenza Portici snc, Milano Due, 20090 Segrate – Milano- Italia

Le informazioni relative alla procedura da seguire per le Segnalazioni sono facilmente accessibili a tutte le persone che potrebbero effettuare una Segnalazione, attraverso la loro pubblicazione sul sito *web* della SIM, in una sezione dedicata, e nella Rete Aziendale.

Ciascuna segnalazione può essere inoltrata in formato anonimo da ciascun Segnalante (condizione non obbligatoria, nel caso in cui il Segnalante intendesse rivelare la propria identità, lo fa consapevolmente), indipendentemente dall'inquadramento, dalle mansioni e dall'anzianità. Restano ovviamente ferme le responsabilità di ciascun Segnalante come citate nel paragrafo 10.

Al fine di assicurare la corretta tracciabilità di tutte le segnalazioni pervenute, la Segnalazione comunque pervenuta viene registrata manualmente nell'apposito registro delle segnalazioni mantenuto dal Responsabile della Segnalazione.

Alla segnalazione interna inoltrata è assicurata la massima riservatezza. Il canale di segnalazione è diretto tra il Segnalante e il soggetto incaricato ricevente, senza passaggi o fasi intermedie. Il Responsabile della Segnalazione ha caratteristiche di autonomia e indipendenza rispetto alla Direzione aziendale ovvero ai Responsabili delle varie unità organizzative.

15. Responsabile del Sistema di segnalazione interna o Organismo Ricevente

Ai fini della presente *policy* i destinatari di ciascuna segnalazione interna sono rappresentati da un Amministratore Indipendente e dal Responsabile della Funzione Compliance.

La scelta di identificare un Amministratore Indipendente e il Responsabile della Funzione *Compliance* quali Responsabili della Segnalazione persegue la necessità di garantire il rispetto dei requisiti di autonomia, indipendenza, imparzialità, professionalità e continuità di azione tali da evidenziare eventuali comportamenti ritrosivi nei confronti del Segnalante.

L'Amministratore Indipendente e il Responsabile della Funzione *Compliance*, pur nel rispetto della riservatezza della segnalazione e garantendo l'anonimato del Segnalante e del Segnalato, possono svolgere autonomamente verifiche o approfondimenti sulle circostanze richiamate nella segnalazione, ovvero possono coinvolgere le altre Funzioni del Sistema dei Controlli

Interni o richiedere l'intervento di professionisti esterni. Parimenti, all'Amministratore Indipendente e al Responsabile della Funzione *Compliance* sono attribuite responsabilità per l'informativa alle Autorità di vigilanza e/o con alle Autorità pubblica in caso di gravi irregolarità.

L'Amministratore Indipendente e il Responsabile della Funzione *Compliance* possono accedere alla Segnalazione, attraverso una *username* e una *password*, per la decriptazione dei contenuti della Segnalazione ed avviare, innanzitutto, una valutazione preliminare avente lo scopo di decidere se attivare la fase successiva di vera e propria istruttoria, oppure chiudere la Segnalazione.

Tutte le Segnalazioni effettuate sulla Piattaforma vengono automaticamente riportate nel Registro delle Segnalazioni, nel quale sono archiviate, con un codice progressivo, le Segnalazioni ricevute e le relative e conseguenti azioni poste in essere, sino alla loro chiusura, indicando sempre il motivo secondo il quale ogni Segnalazione si possa ritenere risolta.

16. Esame delle Segnalazioni

Il Responsabile della Segnalazione deve verificare la fondatezza della Segnalazione e la relativa credibilità.

Le persone coinvolte nella Segnalazione possono essere sentite o, a loro richiesta, devono essere sentite, anche attraverso documentazione scritta.

Ai fini della presente procedura, non sono prese in carico le Segnalazioni non fondate da fatti, ovvero indizi precisi e concordanti e aventi mera finalità delatoria a carico del soggetto segnalato. Nell'ambito della gestione del canale di segnalazione interna, il Responsabile della Segnalazione svolge le seguenti attività:

- Rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
- Mantiene le interlocuzioni con la persona segnalante e può richiedere a quest'ultima, se necessario, integrazioni;
- Dà diligente seguito alle segnalazioni ricevute;
- Fornisce 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.

17. Chiusura dell'istruttoria ed attuazione delle azioni definite in fase di analisi delle Segnalazioni

Al termine dell'istruttoria, il Responsabile della Segnalazione indica, sempre nella Piattaforma Whistleblowing, l'esito della stessa, cioè il risultato finale dell'approfondimento dei fatti segnalati.

Se la segnalazione è stata inviata a un soggetto interno diverso dal Responsabile della Segnalazione e questa viene considerata "segnalazione whistleblowing" va trasmessa, entro sette giorni dal suo ricevimento, al soggetto interno competente, dandone contestuale notizia della trasmissione alla persona segnalante. In caso contrario la stessa potrebbe essere considerata ordinaria.

Qualora la Segnalazione risulti fondata, il Responsabile della Segnalazione provvede a darne comunicazione al Consiglio di Amministrazione. A tale comunicazione scritta devono essere allegati le relative evidenze a supporto dell'attività di verifica effettuata. In caso di accertata fondatezza di una Segnalazione, la Società adotterà gli eventuali provvedimenti ritenuti opportuni e le azioni a tutela della Società. Nel caso gli illeciti rientrino in quelli previsti dal Modello Organizzativo 231/01 il Responsabile della Segnalazione dovrà analizzare la stessa mediante la collaborazione dell'OdV. In tal caso si applicherà il sistema sanzionatorio ivi incluso nel Modello stesso

L'OdV riepiloga annualmente le Segnalazioni relative ai reati citati nel Modello 231 nell'ambito della propria relazione.

18. Conservazione della documentazione

La documentazione relativa alle segnalazioni interne ed esterne deve essere conservata per il tempo necessario al loro trattamento e comunque non oltre cinque anni dalla data di comunicazione dell'esito della segnalazione, nel rispetto degli obblighi stabiliti dal D. lgs. n. 24/2023 e dei principi dettati dal GDPR.