

Policy Whistleblowing

VERSIONE	DATA DOCUMENTO	VALIDATO DA
1.0	24/10/2019	Consiglio di Amministrazione
2.0	30/01/2025	Consiglio di Amministrazione

Indice

1. PREMESSA E DEFINIZIONI	3
2. RIFERIMENTI NORMATIVI	4
3. NOMINA DEL RESPONSABILE DEI SISTEMI DI SEGNALAZIONE INTERNI	5
4. MODALITÀ DI SEGNALAZIONE	5
4.1 Contenuto della segnalazione	7
4.2 Procedure di segnalazione	8
4.3 Provvedimenti decisionali.....	9
5. SEGNALAZIONI ESTERNE ALLE AUTORITA' DI VIGILANZA	9
6. FORME DI TUTELA ADOTTATE DALLA SIM	10
6.1 Protezione del soggetto segnalante	10
6.1.1 Tutela dell'anonimato	10
6.1.2 Divieto di discriminazione.....	10
6.2 Protezione dei dati e archiviazione dei documenti.....	11
7. RESPONSABILITÀ DEL SOGGETTO SEGNALANTE	11
8. RELAZIONE ANNUALE	11
ALLEGATI	12

1. Premessa e definizioni

1.1 Premessa

La SIM promuove una cultura aziendale caratterizzata da comportamenti corretti e da un buon sistema di *corporate governance*, quindi, considera il Whistleblowing un importante strumento per prevenire, evitare o interrompere azioni illecite potenzialmente dannose e promuovere, al tempo stesso, trasparenza ed integrità. Per tale ragione, la presente *Policy* definisce le modalità di comunicazione per la ricezione, l'analisi ed il trattamento delle segnalazioni di comportamenti illegittimi (c.d. "*whistleblowing*").

Per comportamento illegittimo si intende qualsiasi azione o omissione, avvenuta nello svolgimento dell'attività lavorativa o che abbia un impatto sulla stessa, che arrechi o che possa arrecare danno o pregiudizio alla SIM e/o ai suoi Dipendenti e che:

- sia illecita, scorretta o immorale;
- violi le disposizioni normative e regolamentari; o
- non sia conforme alle normative interne.

La presente *Policy* si applica a

- tutti i dipendenti della SIM;
- consulenti finanziari abilitati all'offerta fuori sede;
- lavoratori autonomi e titolari di un rapporto di collaborazione, lavoratori o collaboratori di fornitori, liberi professionisti e consulenti che prestano la propria attività presso la SIM;
- volontari e tirocinanti (retribuiti e non retribuiti);
- azionisti e persone con funzioni di amministrazione, direzione, controllo e vigilanza o rappresentanza;
- candidati;
- lavoratori in prova;
- ex lavoratori.

In linea con le previsioni della normativa esterna, Euclidea SIM garantisce la riservatezza dei dati personali del segnalante, nonché la tutela da eventuali condotte ritorsive di contenuto professionale, contrattuale od organizzativo e da qualsiasi azione od omissione che possa realizzare una forma di ritorsione, penalizzazione o discriminazione diretta o indiretta a suo carico per motivi collegati, direttamente o indirettamente, alla segnalazione effettuata. Le misure di protezione vengono inoltre estese anche ai soggetti terzi coinvolti.

In tale ambito, la presente *Policy* è volta a declinare idonee soluzioni organizzative in conformità a quanto previsto dalle disposizioni normative e proporzionalmente al profilo dimensionale e alla complessità operativa della SIM.

Il sistema interno di segnalazione delle violazioni adottato dalla SIM è sottoposto ad approvazione del Consiglio di Amministrazione.

1.2 Definizioni

- **Canali di segnalazione:** sistemi diversificati previsti dal Decreto per la presentazione delle Segnalazioni: (i) Canale interno; (ii) Canale esterno presso ANAC; (iii) Divulgazione pubblica;
- **Canale interno per la Segnalazione:** piattaforma informatica denominata Whistleblowing fornita da Ascofind, utilizzabile per effettuare le Segnalazioni interne;
- **Canale esterno per la Segnalazione:** piattaforma ANAC;
- **Contesto lavorativo:** le attività lavorative o professionali, presenti o passate, svolte dal Personale di Euclidea 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 Decreto Legislativo;
- **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 delle segnalazioni;
- **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;
- **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 della SIM:** coloro che sono legati a Euclidea SIM da un rapporto di lavoro subordinato o di prestazione occasionale nonché i Vertici aziendali e i componenti degli organi sociali della SIM;
- **Segnalante:** la persona che effettua una Segnalazione tramite il canale di Segnalazione interno o esterno, denuncia, Divulgazione pubblica; definito anche come Whistleblower;
- **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 esterna:** la comunicazione, scritta od orale, di Informazioni sulle violazioni effettuata dal Segnalante tramite il canale di segnalazione esterno attivato dall'Autorità Nazionale Anticorruzione (ANAC);
- **Segnalazione interna:** la comunicazione, scritta o orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interno.

2. Riferimenti normativi

- Decreto Legislativo 24 febbraio 1998, n. 58 e s.m.i ("TUF");
- "Regolamento di attuazione degli articoli 4 – undecies e 6, comma 1, lettere b) e c-bis), del TUF" (adottato dalla Banca d'Italia con Provvedimento del 5 dicembre 2019, come modificato dal Provvedimento di Banca d'Italia del 23 dicembre 2022), art. 9 e "Allegato 4";

- Decreto Legislativo del 10 marzo 2023, n. 24 (c.d. “Decreto Whistleblowing”);
- Decreto Legislativo 21 novembre 2007, n. 231, modificato e integralmente riscritto dal Decreto Legislativo 25 maggio 2017, n. 90 (“Decreto Antiriciclaggio).

3. Nomina del Responsabile dei sistemi di segnalazione interni

Conformemente con quanto previsto dalle disposizioni normative, la SIM ha individuato nel Consigliere indipendente il Responsabile dei sistemi interni di segnalazione con il compito di:

- assicurare il corretto svolgimento del procedimento di segnalazione;
- ricevere, esaminare e valutare le segnalazioni ricevute;
- riferire direttamente e senza indugio al Consiglio di Amministrazione e al Collegio Sindacale le informazioni oggetto di segnalazione, ove rilevanti;
- redigere una relazione annuale sul corretto funzionamento del sistema interno di segnalazione, contenente informazioni aggregate sulle risultanze dell’attività svolta a seguito delle segnalazioni ricevute, da sottoporre ad approvazione del Consiglio di Amministrazione e mettere a disposizione del personale;
- tenere apposito registro delle segnalazioni ricevute e dei relativi esiti.

La SIM, coerentemente con le previsioni normative – alla luce del principio di proporzionalità – e con il proprio modello organizzativo e operativo, ha ritenuto di attribuire al Responsabile dei sistemi di segnalazione anche le attività di ricezione, nonché quelle di esame e valutazione delle segnalazioni¹. Tale attività di esame e di valutazione potrà essere effettuata da parte del Responsabile anche con il supporto, se necessario, di personale qualificato anche esterno.

Il Responsabile deve essere in possesso dei requisiti previsti dalle disposizioni applicabili (i.e. non deve essere gerarchicamente o funzionalmente subordinato al soggetto eventualmente segnalato, e non deve partecipare all’adozione degli eventuali provvedimenti decisionali, che sono rimessi alle funzioni o agli organi aziendali competenti).

Qualora il Responsabile dei sistemi interni, nonché della ricezione, esame e valutazione delle segnalazioni, sia il presunto responsabile della violazione o abbia un potenziale interesse correlato alla segnalazione tale da compromettere l’imparzialità di giudizio, le attività di ricezione, esame e valutazione delle segnalazioni sono svolte dalla “Funzione di Riserva”, individuata dal Consiglio di Amministrazione nel responsabile della Funzione di Internal Audit.

4. Modalità di segnalazione

La segnalazione deve contenere le informazioni previste dal modello riportato in allegato alla presente *Policy* ed è inviata dal soggetto segnalante al Responsabile dei sistemi interni attraverso una delle seguenti modalità:

- a) mediante inserimento della segnalazione attraverso il sito web della SIM accessibile attraverso il link <https://www.euclidea.com/whistleblowing/>. La Piattaforma è fornita da ASCOFIND ed assicura la

¹ Ai sensi dell’“Allegato 4” al Regolamento emanato dalla Banca d’Italia con Provvedimento del 5 dicembre 2019, “*Le attività di ricezione, esame e valutazione delle segnalazioni possono essere esternalizzate nel rispetto della disciplina in materia di esternalizzazione. In caso di esternalizzazione, il fornitore di servizi riferisce al responsabile dei sistemi interni di segnalazione*”.

riservatezza del Segnalante, del Facilitatore, della persona coinvolta o comunque dei soggetti menzionati nella segnalazione, del contenuto della segnalazione e della relativa documentazione.

Digitato l'indirizzo web sopra indicato, i destinatari della procedura potranno:

- attraverso il pulsante INVIA UNA SEGNALAZIONE avviare il processo di Segnalazione;
 - selezionare l'area riservata ad Euclidea SIM;
 - compilare il FORM che prevede: campi descrittivi liberi, campi a risposta multipla oltre alla possibilità di allegare files;
 - completare la segnalazione;
 - inviare la segnalazione
 - modificare o aggiornare una segnalazione inviata;
 - mantenere riservato il contenuto della segnalazione durante l'intera fase di gestione della stessa, consentendo l'accesso ai soli soggetti autorizzati;
 - consultare lo stato di una segnalazione inviata;
 - ricevere riscontro sugli esiti delle verifiche.
- b) mediante invio all'apposito indirizzo *e-mail* whistleblowing@euclidea.com, riconducibile al soggetto preposto alla ricezione della segnalazione. Qualora tale soggetto sia il presunto responsabile della violazione o abbia un potenziale interesse correlato alla segnalazione, tale da compromettere l'imparzialità di giudizio, tramite l'indirizzo *e-mail* della "Funzione di Riserva" come sopra individuata;
- c) tramite lettera raccomandata all'indirizzo Euclidea SIM - Via Laura Solera Mantegazza, 7, 20121 Milano MI, all'attenzione personale del soggetto preposto alla ricezione della segnalazione "Responsabile Whistleblowing" come sopra individuato. Qualora tale soggetto sia il presunto responsabile della violazione o abbia un potenziale interesse correlato alla segnalazione tale da compromettere l'imparzialità di giudizio, all'indirizzo Euclidea SIM - Via Laura Solera Mantegazza, 7, 20121 Milano MI, all'attenzione personale della "Funzione di Riserva" come sopra individuata;
- d) in alternativa alle modalità precedenti, tramite canale esterno utilizzando la modalità attiva presso ANAC <https://whistleblowing.anticorruzione.it/#/>.

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

In ogni caso, l'identità del segnalante sarà conosciuta solo dal Responsabile dei sistemi interni che ne garantisce la riservatezza, fatti salvi i casi in cui le informazioni siano necessarie per le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione.

Per incentivare l'uso dei sistemi interni di segnalazione e favorire la diffusione di una cultura della legalità, sono illustrati al personale in maniera chiara, precisa e completa il procedimento di segnalazione interno, i presidi posti a garanzia della riservatezza dei dati personali del segnalante e del presunto responsabile della violazione. Il personale è avvertito che le disposizioni di legge europee e nazionali in materia di protezione dei dati personali che regolano l'accesso ai dati personali non trovano 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.

Dovrà altresì essere garantita la tutela adeguata del soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione.

Il presunto responsabile della violazione è tutelato da ripercussioni negative derivanti dalla segnalazione nel caso in cui dal procedimento di segnalazione non emergano elementi che giustificano l'adozione di provvedimenti nei suoi confronti².

Tipologie di irregolarità che possono essere segnalate

Il nuovo Decreto definisce ed estende le violazioni che possono essere segnalate in comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità della SIM, di cui si siano venute a conoscenza nel contesto lavorativo, e che consistono in illeciti amministrativi, contabili, civili o penali. Si riportano di seguito le principali norme la cui violazione può, pertanto, essere oggetto di segnalazione:

- norme disciplinanti le attività della SIM;
- norme disciplinanti l'attività finanziaria;
- norme in materia di prevenzione del riciclaggio e del finanziamento del terrorismo;
- modello di Organizzazione e Gestione ex D.lgs. 231/01;
- leggi antitrust; violazioni che implicano l'avvio di un procedimento disciplinare, previsto dalla legislazione sul lavoro o dai contratti collettivi e individuali applicabili;
- violazioni suscettibili di arrecare un danno patrimoniale o innescare un rischio reputazionale a Euclidea SIM;
- norme, leggi e regolamenti, Codici di Comportamento o altre disposizioni aziendali.

4.1 Contenuto della segnalazione

Il segnalante deve fornire, fin ove possibile, gli elementi utili alla ricostruzione del fatto e ad accertare la fondatezza di quanto segnalato. A tal fine, la segnalazione deve contenere i seguenti elementi:

- nome e cognome del soggetto che effettua la segnalazione ("segnalante"), con espressa indicazione dell'inquadramento e della qualifica professionale, della sede di lavoro e dei recapiti;
- se noti, la data e il luogo in cui si è verificato il fatto oggetto della segnalazione;
- chiara e completa descrizione dei fatti oggetto di segnalazione;
- generalità o altri elementi che consentano di identificare il soggetto o i soggetti che hanno posto in essere i fatti segnalati;
- eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione ed eventuali documenti che possono confermare la fondatezza di tali fatti;
- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati;
- dichiarazione del segnalante in merito all'assenza o alla sussistenza di un interesse privato collegato alla segnalazione.

² In caso di adozione di provvedimenti nei confronti del responsabile della violazione, costui dovrà essere tutelato da eventuali effetti negativi diversi da quelli previsti dai provvedimenti adottati.

4.2 Procedure di segnalazione

Una volta ricevuta la segnalazione, il Responsabile dei sistemi interni (ovvero la “Funzione di Riserva” qualora ricorrano i presupposti) comunica, entro 10 giorni, al segnalante (attraverso la stessa modalità di ricezione della segnalazione) l'avvio del procedimento di esame e dà inizio alla verifica della fondatezza o meno della segnalazione.

Nel corso del processo di analisi, il Responsabile dei sistemi interni effettua la valutazione della segnalazione in termini di rilevanza e gravità della stessa e, nel caso in cui la stessa risulti essere fondata, provvede a:

- definire un apposito piano di intervento;
- informare il segnalante (attraverso la stessa modalità di ricezione della segnalazione) e il segnalato (tramite comunicazione separata), circa gli esiti della valutazione stessa;
- informa tempestivamente il Consiglio di Amministrazione ed il Collegio Sindacale nei casi in cui si siano verificate violazioni di particolari gravità, nonché il Direttore Generale e l'Ufficio Personale affinché valutino l'eventuale adozione di provvedimenti di competenza, incluso, ove sussistano i presupposti, l'esercizio dell'azione disciplinare.

Qualora oggetto della segnalazione sia il medesimo Responsabile dei sistemi interni di segnalazione e la segnalazione venga ritenuta fondata e rilevante, in via del tutto eccezionale l'informativa tempestiva agli Organi Aziendali dovrà essere fornita direttamente dalla “Funzione di Riserva”.

Diversamente, nel caso di infondatezza della segnalazione, il Responsabile dei sistemi interni comunica al segnalante (attraverso la stessa modalità di ricezione della segnalazione) l'esito motivato e la conclusione del procedimento.

Al termine dell'indagine, il responsabile dei sistemi interni predispone una relazione all'interno della quale sono riportate:

- l'iter dell'indagine e le prove raccolte;
- le conclusioni alle quali si è giunti;
- le raccomandazioni e le azioni da porre in essere per sopperire alle violazioni riscontrate ed assicurare che queste non si verifichino in futuro.

In qualunque fase del procedimento – e senza attendere l'esito della valutazione – il Responsabile dei sistemi interni riferisce direttamente e senza indugio le informazioni rilevanti oggetto della segnalazione agli Organi Aziendali che provvedono, ove risulti necessario, ad adottare i relativi provvedimenti, anche d'urgenza, ivi incluso, se del caso, l'informativa al Responsabile Antiriciclaggio qualora ricorrano i presupposti per la segnalazione di un'Operazione Sospetta.

La procedura di segnalazione – dalla fase di ricezione alla fase di informativa agli Organi Aziendali – deve essere conclusa nel più breve tempo possibile secondo criteri che tengano conto della gravità della violazione, al fine di prevenire che il perdurare delle violazioni produca ulteriori aggravamenti per la SIM. In ogni caso, la procedura deve concludersi entro 2 mesi dalla ricezione della stessa.

Il processo sin qui descritto deve essere concluso nel più breve tempo possibile, secondo criteri che tengano conto della gravità della violazione, al fine di prevenire che il perdurare delle violazioni produca ulteriori aggravamenti per la SIM. Solo in casi eccezionali e opportunamente motivati, l'esame e la valutazione della segnalazione possono estendersi fino a 4 mesi, previa apposita comunicazione al Collegio Sindacale e al Consiglio di Amministrazione.

4.3 Provvedimenti decisionali

Nel caso in cui le segnalazioni comportino l'assunzione di provvedimenti decisionali, gli stessi sono rimessi al Consiglio di Amministrazione, sentito il Collegio Sindacale.

Nel caso in cui il segnalante sia corresponsabile della violazione oggetto di segnalazione, il Consiglio di Amministrazione, sentito il Collegio Sindacale, prevede un trattamento privilegiato nei suoi confronti rispetto agli altri corresponsabili, salvi i casi in cui la condotta del segnalante risulti di particolare e critica gravità.

5. Segnalazioni esterne alle Autorità di Vigilanza

Ai sensi dell'art. 4-duodecies del TUF, il personale della SIM può effettuare le segnalazioni anche direttamente alle Autorità di Vigilanza in conformità alle regole operative da loro definite ("Segnalazioni Esterne").

A tal proposito, Banca d'Italia e Consob:

- a) ricevono, ciascuna per le materie di propria competenza, da parte del personale che può effettuare segnalazioni ai sensi della presente procedura, segnalazioni che si riferiscono a violazioni delle norme del TUF, e delle relative disposizioni di attuazione, nonché di atti dell'Unione europea direttamente applicabili nelle stesse materie;
- b) possono stabilire condizioni, limiti e procedure per la ricezione delle segnalazioni, tenendo conto:
 - 1. della riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione; l'identità del segnalante è sottratta all'applicazione dell'art. 7, comma 2, del Decreto Legislativo 30 giugno 2003, n. 196, e non può essere rivelata per tutte le fasi della procedura, salvo suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato;
 - 2. della tutela adeguata del soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
- c) si avvalgono delle informazioni contenute nelle segnalazioni, ove rilevanti, esclusivamente nell'esercizio delle funzioni di vigilanza;
- d) prevedono, mediante protocollo d'intesa, le opportune misure di coordinamento nello svolgimento delle attività di rispettiva competenza, ivi compresa l'applicazione delle relative sanzioni, in modo da coordinare l'esercizio delle funzioni di vigilanza e ridurre al minimo gli oneri gravanti sui soggetti vigilati.

Gli atti relativi alle segnalazioni sono sottratti all'accesso previsto dagli artt. 22 e ss. della Legge 7 agosto 1990, n. 241, e successive modificazioni.

Sul sito della Consob è possibile consultare la sezione dedicata, al seguente indirizzo <http://www.consob.it/web/area-pubblica/whistleblowing>.

In tale sezione sono indicate le modalità operative che tutto il personale della SIM deve seguire per trasmettere direttamente alla Consob segnalazioni riferite a presunte violazioni o illeciti delle norme del TUF, nonché di atti dell'Unione europea direttamente applicabili nelle stesse materie.

Analogamente la Banca d'Italia ha attivato due canali telematici dedicati alla ricezione delle segnalazioni aventi a oggetto esclusivamente possibili violazioni normative o presunte irregolarità gestionali riscontrate presso intermediari vigilati.

I dipendenti e i collaboratori della SIM possono inviare le segnalazioni alla casella di posta elettronica whistleblowing-vigilanza@bancaditalia.it, o, in alternativa, tramite posta ordinaria secondo le modalità descritte nella sezione dedicata del sito web <https://www.bancaditalia.it/compiti/vigilanza/whistleblowing>.

In conformità alla normativa in materia (art. 52-ter TUB, art. 4-duodecies TUF e legge 30 novembre 2017, n. 179), la Banca d'Italia assicura la riservatezza dei dati personali del segnalante.

6. Forme di tutela adottate dalla SIM

6.1 Protezione del soggetto segnalante

6.1.1 Tutela dell'anonimato

Al fine di evitare che il timore di subire conseguenze pregiudizievoli possa indurre a non segnalare le violazioni di cui al punto 1, l'identità del segnalante (*whistleblower*) non può essere rivelata senza il suo espresso consenso e tutti coloro che ricevono o sono coinvolti nella gestione delle segnalazioni sono tenuti a tutelare la riservatezza di tale informazione.

Fanno eccezione le 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'art. 2043 c.c., nonché le ipotesi in cui l'anonimato non sia opponibile per legge (quando, ad esempio, le informazioni siano necessarie per lo svolgimento di indagini penali, tributarie o amministrative, oppure per le ispezioni degli organi di controllo).

L'anonimato del *whistleblower* è altresì garantito nell'ambito del procedimento disciplinare quando la contestazione al segnalato sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione (ipotesi che può verificarsi nei casi in cui la segnalazione è solo uno degli elementi che hanno fatto emergere l'illecito, mentre la contestazione disciplinare viene mossa sulla base di altri fatti da soli sufficienti a giustificare l'apertura del procedimento disciplinare).

La SIM garantisce l'anonimato del segnalante, ad eccezione dei casi in cui:

- il segnalante esprima il proprio consenso alla divulgazione;
- la sua divulgazione sia richiesta dalla normativa locale (ad esempio, se sia necessario coinvolgere la polizia o le Autorità, ovvero se il segnalato abbia il diritto di riceverne notifica);
- la sua divulgazione sia necessaria per prevenire o ridurre minacce a danno della salute o della sicurezza delle persone o per la difesa del segnalato.

La divulgazione non autorizzata dell'identità del segnalante o di informazioni in base alle quali si possa dedurre, è considerata una violazione della presente *Policy* ed è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

6.1.2 Divieto di discriminazione

Il soggetto che effettua una segnalazione non può essere sanzionato, licenziato o sottoposto a condotte ritorsive o discriminatorie³, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati, anche indirettamente, alla segnalazione. Per misure discriminatorie si intendono le azioni disciplinari ingiustificate, le molestie sul luogo di lavoro ed ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili.

Nei casi più gravi, e qualora sia possibile, il soggetto segnalante ha il diritto di chiedere il trasferimento in altro ufficio e, laddove necessario, l'assistenza psicologica indipendente in caso di *stress* derivante dalla segnalazione.

Il soggetto che ritiene di aver subito una discriminazione ne dà notizia circostanziata al Responsabile dei sistemi interni di segnalazione, che, una volta valutata la fondatezza, segnala l'ipotesi di discriminazione all'Amministratore Delegato e al Direttore Generale, al fine di consentire l'adozione dei provvedimenti necessari a ripristinare la situazione e/o rimediare agli effetti negativi della discriminazione.

È vietata, altresì, ogni forma di ritorsione o discriminazione avente effetti sulle condizioni di lavoro di chi collabora alle attività di riscontro della fondatezza della segnalazione.

³ Per misure discriminatorie si intendono le azioni disciplinari ingiustificate, le molestie sul luogo di lavoro ed ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili.

6.2 Protezione dei dati e archiviazione dei documenti

Al fine di assicurare la ricostruzione delle differenti fasi del processo di segnalazione, è cura del Responsabile dei sistemi interni garantire:

- la tracciabilità delle segnalazioni e delle relative attività istruttorie;
- la conservazione della documentazione inerente le segnalazioni e le relative attività di verifica, in appositi archivi (cartacei/informatici), con gli opportuni livelli di sicurezza e riservatezza;
- la conservazione della documentazione e delle segnalazioni per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati e comunque nel rispetto delle procedure *privacy* vigenti nella SIM.

La gestione dei dati personali avviene nel rispetto degli obblighi di riservatezza stabiliti dall'articolo 12 del Decreto Legislativo e in conformità con la normativa sulla protezione dei dati personali, come specificato 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 tutela dei dati personali è estesa non solo al Segnalante (nelle segnalazioni non anonime) ma anche alle persone coinvolte o menzionate nella segnalazione.

7. Responsabilità del soggetto segnalante

La presente *Policy* lascia impregiudicata la responsabilità penale e disciplinare del *whistleblower* nell'ipotesi di segnalazione calunniosa o diffamatoria ai sensi del codice penale (artt. 368 e 595 c.p.) e dell'art. 2043 c.c.

Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso del presente regolamento, quali le segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il segnalato e/o altri soggetti, ed ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto del presente documento.

8. Relazione annuale

Il Responsabile dei sistemi interni redige annualmente, nel rispetto della tutela dei segnalanti, una relazione sul corretto funzionamento dei sistemi interni di segnalazione contenente le informazioni sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute.

Tale relazione è approvata dal Consiglio di Amministrazione - sentito il Collegio Sindacale – e messa a disposizione del personale.

Allegati

MODELLO PER LA SEGNALAZIONE DELLE VIOLAZIONI	
NOME E COGNOME DEL SEGNALANTE	
INQUADRAMENTO E QUALIFICA PROFESSIONALE	
SEDE DI LAVORO	
TELEFONO/CELLULARE	
E-MAIL	
DATA/PERIODO IN CUI SI E' VERIFICATO IL FATTO	
LUOGO FISICO IN CUI SI E' VERIFICATO IL FATTO	<input type="checkbox"/> UFFICIO (Indicare denominazione e indirizzo della struttura) _____ <input type="checkbox"/> ALL'ESTERNO DELL'UFFICIO (Indicare luogo e indirizzo) _____
COMPLETA DESCRIZIONE DEGLI ATTI O DEI FATTI	
PRESUNTO/I AUTORE/I DEGLI ATTI O DEI FATTI	
PRESUNTI ALTRI EVENTUALI SOGGETTI A CONOSCENZA DEGLI ATTI O DEI FATTI E/O IN GRADO DI RIFERIRE SUL MEDESIMO	
EVENTUALI ULTERIORI INFORMAZIONI UTILI AI FINI DELLA SUSSISTENZA DEI FATTI/ATTI SEGNALATI	
EVENTUALI ALLEGATI A SOSTEGNO DELLA SEGNALAZIONE	

Il sottoscritto _____ dichiara l'assenza di qualsiasi interesse privato collegato alla segnalazione.

oppure

Il sottoscritto _____ dichiara la sussistenza di un interesse privato collegato alla dichiarazione, di seguito evidenziata (*Descrizione dell'interesse*)

 Luogo, data