

POLICY IN MATERIA DI WHISTLEBLOWING

Redazione	Amministratore Delegato/Consulente incaricato
Verifica	Amministratore Delegato Responsabile Funzione <i>Compliance</i>
Data di approvazione	Consiglio di Amministrazione del 29/06/2022
Revisione	Rev. 01 del 26/02/2025

INDICE

1. PREMESSA	3
2. IL QUADRO NORMATIVO DI RIFERIMENTO	3
3. AMBITO DI APPLICAZIONE	4
4. NOMINA DEL RESPONSABILE DEI SISTEMI INTERNI DI SEGNALAZIONE	5
5. CONTENUTO E MODALITÀ DI SEGNALAZIONE	6
5.1 <i>Segnalazioni interne delle violazioni</i>	6
5.2 <i>Segnalazioni alle Autorità di Vigilanza</i>	7
5.3 <i>Segnalazioni all’A.N.A.C.</i>	8
5.4 <i>Divulgazione pubblica</i>	9
6. PROCEDURA DI SEGNALAZIONI INTERNE	9
7. FORME DI TUTELA DEL SEGNALANTE	11
7.1 <i>Tutela dell’anonimato</i>	11
7.2 <i>Divieto di discriminazione</i>	11
8. RESPONSABILITÀ DEL SEGNALANTE	12
9. PROTEZIONE DEI DATI E ARCHIVIAZIONE DEI DOCUMENTI	12
10. AGGIORNAMENTO DELLA POLICY	12
ALLEGATO A – Modulo per la segnalazione interna delle violazioni	13
ALLEGATO B – Informativa per il dipendente soggetto a investigazione interna	14

1. PREMESSA

Equiter SGR S.p.A. (di seguito anche la “**SGR**” o la “**Società**”) si impegna costantemente a condurre la propria attività con onestà e integrità. Tuttavia, va riconosciuto il fatto che ogni azienda è soggetta al rischio di azioni scorrette o comportamenti illeciti.

È quindi dovere della SGR adottare misure adeguate a identificare tali situazioni al fine di porvi rimedio. Incoraggiando a livello aziendale una cultura aperta e responsabile, è possibile inoltre contribuire a prevenire le stesse situazioni.

Tutto il personale della Società è tenuto ad osservare le procedure e le *policy* adottate dalla SGR e a segnalare qualsiasi comportamento che non rispetti i principi fondamentali in esso contenuti.

Ogni singolo soggetto ha la responsabilità di esprimere eventuali timori su possibili condotte illecite nell’ambito del contesto lavorativo.

2. IL QUADRO NORMATIVO DI RIFERIMENTO

Nell’ambito delle disposizioni che disciplinano l’attività svolta dagli intermediari, a seguito dell’entrata in vigore del Decreto Legislativo del 3 agosto 2017, n. 129, sono stati introdotti nel Decreto Legislativo del 24 febbraio 1998, n. 58 (Testo Unico della Finanza, di seguito anche “**TUF**”) l’articolo 4-undecies “*Sistemi interni di segnalazione delle violazioni*” e l’articolo 4-duodecies “*Procedura di segnalazione alle Autorità di Vigilanza*” che hanno esteso l’ambito di applicazione delle segnalazioni interne alla SGR (c.d. *whistleblowing*), da parte del personale, agli atti o fatti che possano costituire violazioni delle norme disciplinanti l’attività svolta, nonché del Regolamento (UE) n. 596/2017 (“**Market Abuse**”).

La Banca d’Italia e la Consob adottano, secondo le rispettive competenze, le disposizioni attuative, avuto riguardo all’esigenza di coordinare le funzioni di vigilanza e ridurre al minimo gli oneri gravanti sui soggetti destinatari.

In particolare, con l’adozione del Provvedimento del 5 dicembre 2019 recante il “*Regolamento della Banca d’Italia di attuazione degli articoli 4-undecies e 6, comma 1, lettere b) e c-bis) del TUF*” (di seguito anche “**Regolamento della Banca d’Italia**”), la Banca d’Italia ha stabilito che gli organi di supervisione strategica delle SGR devono approvare i sistemi interni di segnalazione delle violazioni secondo quanto previsto dall’Allegato 4 del medesimo Regolamento.

Con riferimento alle disposizioni in materia di “*Antiriciclaggio*”, il 4 luglio 2017 è entrato in vigore il Decreto Legislativo del 25 maggio 2017, n. 90 che ha modificato e riscritto integralmente, anziché emendarlo, il contenuto del Decreto Legislativo del 21 novembre 2007, n. 231 (di seguito anche “**D. Lgs. n. 231/2007**”). L’articolo 48 del Capo VII (“*segnalazioni di violazioni*”) del nuovo D.Lgs. n.231/2007 prevede l’introduzione del sistema di segnalazione di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo (c.d. *whistleblowing*). Tali disposizioni normative mirano a definire i requisiti minimi necessari per la predisposizione di sistemi di *whistleblowing*, volti a consentire al personale di segnalare atti e fatti che possano costituire una violazione delle norme che regolano il contrasto al riciclaggio e al finanziamento del terrorismo, garantendo al contempo la riservatezza e la protezione dei dati personali del soggetto che effettua la segnalazione e del soggetto segnalato.

Inoltre, la Legge 30 novembre 2017, n. 179 (rubricato «Tutela del dipendente o collaboratore che segnala illeciti nel settore privato») è intervenuta sul D.lgs. 231/2001 inserendo all'art. 6 (rubricato «Soggetti in posizione apicale e modelli di organizzazione dell'ente») una nuova previsione che inquadra nell'ambito del modello di organizzazione e gestione di cui al Decreto le misure legate alla presentazione e gestione di segnalazioni di condotte illecite rilevanti ai sensi del D.lgs. 231/2001 e di violazioni del Modello, nonché le relative forme di tutela del segnalante.

Il D.lgs. 10 marzo 2023, n. 24 ha abrogato l'art. 6, comma 2-bis, lett. a) del D.lgs. 231/2001, regolamentando in modo organico la disciplina in materia di segnalazione *whistleblowing*. In particolare, il D.lgs. citato recepisce la direttiva comunitaria (UE) 2019/1937 sul punto ed estende le tutele previste a tutti coloro che segnalano violazioni di cui sono venuti a conoscenza nell'ambito del proprio contesto lavorativo, in qualità di dipendenti o collaboratori, lavoratori subordinati e autonomi, liberi professionisti ed altre categorie come volontari e tirocinanti anche non retribuiti, gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza. Inoltre, le misure di protezione si applicano anche ai cosiddetti "facilitatori", colleghi, parenti o affetti stabili di chi ha segnalato.

Secondo il Decreto 24/2023, le aziende interessate (ossia con più di 50 dipendenti o che abbiano adottato un Modello 231 o che rientrino nell'applicazione delle norme di cui alle parti I.B e II dell'Allegato al Decreto 24/2023) dovranno predisporre canali interni di segnalazione in grado di garantire il massimo livello di riservatezza. Nelle aziende con meno di cinquanta dipendenti viene consentita solo la segnalazione interna escludendo la possibilità di ricorrere al canale esterno e alla divulgazione pubblica.

Tra i suoi contenuti vincolanti la direttiva – interamente recepita dal Decreto attuativo e dal Modello 231 della SGR – prevede che la tutela sia riconosciuta anche in caso di segnalazioni o divulgazioni rivelatesi poi infondate, qualora il segnalante abbia avuto fondati motivi di ritenere che le violazioni fossero vere. La tutela cessa però nel caso in cui le segnalazioni infondate siano state effettuate con dolo o colpa grave.

È altresì prevista la possibilità di segnalazioni esterne (presso i canali A.N.A.C.) a patto che sia stato preventivamente utilizzato il canale interno e, in particolari casi, la divulgazione pubblica.

3. AMBITO DI APPLICAZIONE

La presente *Policy* si pone l'obiettivo di individuare idonee soluzioni organizzative in materia di *whistleblowing*, in conformità con quanto previsto dalle citate disposizioni normative e proporzionalmente al profilo dimensionale e alla complessità operativa della SGR.

Come sopra riportato, la normativa primaria applicabile alla SGR circoscrive il perimetro oggettivo del *whistleblowing* a:

- ❖ agli *atti o fatti che possano costituire violazione delle norme disciplinanti l'attività svolta, nonché del Regolamento (UE) n. 596/2014*;
- ❖ *alle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo*;
- ❖ illeciti amministrativi, contabili, civili o penali, condotte illecite rilevanti ai sensi del D.lgs. 231/2001 e violazioni del Modello 231.

Inoltre, la SGR ritiene di inserire nell'ambito del perimetro del *whistleblowing* anche quanto definito all'interno del Codice Etico e di Comportamento.

Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del Codice Civile, la presentazione di una segnalazione non costituisce violazione degli obblighi derivanti dal rapporto di lavoro.

Le segnalazioni possono essere effettuate da tutto il personale della SGR, così come definito dall'articolo 1, comma 2, lettera cc) del D.Lgs. n.231/2007 (oltrech  dall'art. 1, comma 1, lett. i-ter) del TUF), ovvero *“i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l’inserimento nell’organizzazione del soggetto obbligato, anche in forma diversa dal rapporto di lavoro subordinato, ivi compresi i consulenti finanziari abilitati all’offerta fuori sede di cui all’articolo 31, comma 2, del TUF nonch  i produttori diretti e i soggetti addetti all’intermediazione di cui all’articolo 109, comma 2, lettere c) ed e), CAP”*. Inoltre, in osservanza con quanto disposto dal D.lgs. 24/2023, possono effettuare segnalazioni: lavoratori autonomi, liberi professionisti e consulenti che svolgono la propria attivit  lavorativa presso la societ ; lavoratori o collaboratori delle imprese fornitrici di beni o servizi; volontari e tirocinanti, retribuiti e non retribuiti; azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.

  possibile segnalare nei seguenti casi:

- quando il rapporto giuridico   in corso;
- quando il rapporto giuridico non   ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
- durante il periodo di prova;
- successivamente allo scioglimento del rapporto giuridico, se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

La SGR   tenuta a fornire la suddetta *Policy* e i successivi aggiornamenti a tutti i dipendenti, nonch  a pubblicarla sul proprio sito *internet*.

Il Consiglio di Amministrazione approva i sistemi interni di segnalazione delle violazioni.

4. NOMINA DEL RESPONSABILE DEI SISTEMI INTERNI DI SEGNALAZIONE

Conformemente con quanto previsto dall'art. 4, comma 2, D.lgs. 24/2023, la SGR designa un Responsabile dei Sistemi Interni di Segnalazione (di seguito anche *“RSIS”*), con il compito di:

- assicurare il corretto funzionamento delle procedure;
- esaminare e valutare le segnalazioni ricevute;
- riferire direttamente e senza indugio al Collegio Sindacale le informazioni oggetto di segnalazione, ove rilevanti;
- redigere – nel rispetto di quanto previsto dalla disciplina sulla protezione dei dati personali – una relazione annuale sul corretto funzionamento del sistema interno di segnalazione, contenente informazioni aggregate sulle risultanze dell'attivit  svolta a seguito delle segnalazioni ricevute. Tale relazione   sottoposta annualmente all'attenzione del Consiglio di Amministrazione.

Il Consiglio di Amministrazione del 26 febbraio 2025 ha nominato l'Organismo di Vigilanza, a esclusione del componente interno, quale soggetto RSIS. Coerentemente con le previsioni normative e con il proprio modello organizzativo e operativo – alla luce del principio di proporzionalità – la SGR ha ritenuto di attribuire al RSIS anche le attività di ricezione, nonché quelle di esame e valutazione delle segnalazioni. Tale attività di esame e di valutazione può essere effettuata da parte del RSIS anche con il supporto, se necessario, di personale qualificato, anche esterno, nel rispetto degli obblighi di riservatezza e in materia di protezione dei dati personali.

Qualora il RSIS sia 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 saranno svolte dal Titolare della "Funzione di riserva", individuata dal Consiglio di Amministrazione del 9 dicembre 2024 nella persona del dott. Roberto Giribaldi, responsabile della Funzione di Internal Audit.

5. CONTENUTO E MODALITÀ DI SEGNALAZIONE

5.1 Segnalazioni interne delle violazioni

Il segnalante (che rientri nella definizione di "personale della SGR" ai sensi di legge e come meglio precisato nel precedente Paragrafo 3) deve fornire, fin ove possibile, gli elementi utili alla ricostruzione del fatto e ad accertare la fondatezza di quanto segnalato. La segnalazione deve contenere i seguenti elementi:

- generalità del soggetto segnalante, con indicazione dell'inquadramento e della qualifica professionale, sede di lavoro e recapiti;
- luogo e data/periodo in cui si è verificato il fatto oggetto di segnalazione;
- descrizione chiara e completa dei fatti oggetto di segnalazione che possano costituire una violazione ai sensi di quanto precisato nel precedente Paragrafo 3;
- 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.

Ai fini della segnalazione, il segnalante è tenuto ad utilizzare il modello riportato in allegato alla presente *Policy* (Allegato A – Modulo per la segnalazione interna delle violazioni).

È comunque indispensabile che i fatti siano di diretta conoscenza del segnalante e non siano stati riferiti da altri soggetti.

La segnalazione è inviata dal segnalante al RSIS attraverso una delle seguenti modalità:

- mediante invio all'apposito indirizzo pec: segnalazioni@equitersgr.it 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: rgiribaldi@regulatoryconsulting.it facente riferimento alla "Funzione di riserva" come sopra individuata;

- tramite posta ordinaria all’indirizzo: piazza San Carlo 156, Torino all’attenzione del “Responsabile dei Sistemi Interni di Segnalazione”, qualora tale soggetto sia il presunto responsabile della violazione o abbia un potenziale interesse collegato alla segnalazione tale da compromettere l’imparzialità di giudizio, al medesimo indirizzo sopra indicato ma all’attenzione della “Funzione di riserva” come sopra individuata. Al fine di garantire la riservatezza del segnalante, è necessario che la segnalazione venga inserita in tre buste chiuse: la prima con il modulo recante i dati identificativi del segnalante; la seconda con il modulo recante la segnalazione, in modo da separare i dati identificativi dalla segnalazione; entrambe le buste dovranno poi essere inserite in una terza busta chiusa che rechi all’esterno la dicitura “Riservata – Al Responsabile dei Sistemi Interni di Segnalazione” ovvero, nei casi suindicati, “Riservata – All’attenzione della Funzione di riserva”.

In ogni caso dovrà essere garantita la 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. Al fine di tutelare la riservatezza del segnalante e la finalità stessa dell’indagine, le informazioni sulla sua identità potranno essere sottratte anche all’esercizio dei diritti previsti dalla normativa in materia di protezione dei dati personali (in particolare artt. 15-22 Regolamento Europeo 2016/679 - GDPR) per tutte le fasi della procedura, salvo suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato. In ogni caso, anche qualora l’identità del segnalante dovesse essere rivelata, ad esempio perché essenziale per la difesa del segnalato, dovrà altresì essere sempre garantita la tutela adeguata del soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione, conformemente a quanto previsto dal D.lgs. 24/2023.

5.2 Segnalazioni alle Autorità di Vigilanza

Dal 3 gennaio 2018, a norma dell’art. 4-*duodecies* del TUF, il personale dei soggetti indicati dall’art. 4-*undecies* del medesimo possono trasmettere le segnalazioni anche direttamente alle Autorità di Vigilanza in conformità a regole operative da loro definite.

A tal proposito, Banca d’Italia e Consob:

- a) ricevono, ciascuna per le materie di propria competenza, da parte del personale dei soggetti indicati al paragrafo 2 della presente *Policy*, segnalazioni che si riferiscono a violazioni delle norme del TUF, 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:
 - 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’articolo 15, comma 1, lettera g), del GDPR, 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;
 - 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 articoli 22 e seguenti della legge 7 agosto 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi", e successive modificazioni.

Alla data di approvazione della presente *policy*, è possibile consultare:

- sul sito della Consob la sezione dedicata, al seguente indirizzo:
<http://www.consob.it/web/area-pubblica/whistleblowing>;
- - sul sito della Banca d'Italia la sezione dedicata, al seguente indirizzo:
<https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/>.

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

5.3 Segnalazioni all'A.N.A.C.

In base a quanto disposto dall'art. 6 del D.lgs. n. 24/2023, la persona segnalante può effettuare una segnalazione esterna all'A.N.A.C. se, al momento della presentazione della stessa, ricorre una delle seguenti condizioni:

- ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- 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;
- ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

La segnalazione esterna è indirizzata all'Autorità Nazionale Anticorruzione (A.N.A.C.) tramite i canali dalla stessa attivati (<https://www.anticorruzione.it/-/whistleblowing>).

Le segnalazioni esterne alle Autorità di Vigilanza per le violazioni delle norme del TUF, nonché di atti dell'Unione direttamente applicabili nelle stesse materie, possono essere effettuate a prescindere dal ricorrere delle condizioni sopra elencate, secondo le modalità indicate nel par. 5.2.

Le segnalazioni esterne possono essere effettuate:

- in forma scritta, tramite la piattaforma informatica, oppure
- in forma orale, attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole.

La segnalazione esterna presentata a un soggetto diverso dall'A.N.A.C. è trasmessa a quest'ultima, entro sette giorni dalla data del suo ricevimento, dando contestuale notizia della trasmissione alla persona segnalante.

L'A.N.A.C. svolge le seguenti attività:

- a) fornisce a qualsiasi persona interessata informazioni sull'uso del canale di segnalazione esterna e del canale di segnalazione interna, nonché sulle misure di protezione previste in materia di *whistleblowing* dal D.lgs. 24/2023;
- b) dà avviso alla persona segnalante del ricevimento della segnalazione esterna entro sette giorni dalla data del suo ricevimento, salvo esplicita richiesta contraria della persona segnalante ovvero salvo il caso in

cui ritenga che l'avviso pregiudicherebbe la protezione della riservatezza dell'identità della persona segnalante;

c) mantiene le interlocuzioni con la persona segnalante e richiede a quest'ultima, se necessario, integrazioni;

d) dà diligente seguito alla segnalazione ricevuta;

e) svolge l'istruttoria necessaria a dare seguito alla segnalazione, anche mediante audizioni e acquisizione di documenti;

f) dà riscontro alla persona segnalante entro tre mesi o, se ricorrono giustificate e motivate ragioni, sei mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei sette giorni dal ricevimento;

g) comunica alla persona segnalante l'esito finale, che può consistere anche nell'archiviazione o nella trasmissione alle autorità competenti o in una raccomandazione o in una sanzione amministrativa.

L'A.N.A.C. dispone, inoltre, l'invio delle segnalazioni aventi ad oggetto informazioni sulle violazioni che non rientrano nella propria competenza alla competente Autorità amministrativa o giudiziaria, ivi comprese le istituzioni, gli organi o gli organismi dell'Unione Europea, e dà contestuale avviso alla persona segnalante dell'avvenuto rinvio. L'Autorità amministrativa competente svolge l'attività di cui alle precedenti lettere c), d), e), f) e g) e garantisce, anche tramite ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

L'A.N.A.C. può non dare seguito alle segnalazioni che riportano violazioni di lieve entità e procedere alla loro archiviazione.

5.4 Divulgazione pubblica

Divulgare pubblicamente vuol dire 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.

La persona segnalante che effettua una divulgazione pubblica beneficia della protezione prevista dal D.lgs. n. 24/2023 se, al momento della divulgazione pubblica, ricorre una delle seguenti condizioni:

- ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro entro i termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
- ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

6. PROCEDURA DI SEGNALAZIONI INTERNE

Conformemente con quanto previsto dall'art. 5 D.lgs. 24/2023, ricevuta la segnalazione, il RSIS (ovvero la "Funzione di riserva" qualora ricorrano i presupposti) comunica, entro 7 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. Le indagini conseguenti alla segnalazione vengono svolte nel

rispetto dei principi di minimizzazione e limitazione della finalità di cui al GDPR, nonché nel rispetto dell'art. 13 D.lgs. 24/2023, e potranno implicare lo svolgimento di indagini puntuali anche sugli strumenti utilizzati per lo svolgimento delle proprie mansioni quali, ad esempio, computer, rete internet, cellulari, ma anche attraverso la visione delle telecamere.

Il segnalato è informato dell'inizio delle indagini a suo carico (Allegato B) salvo che una simile informazione comprometta l'esito dell'indagine. È opportuno documentare simili valutazioni per le quali può essere richiesto il parere del Responsabile della Funzione *Compliance*.

Nel caso in cui si ritenga di non poter informare il segnalato prima dell'indagine, quest'ultimo è in ogni caso informato all'esito della verifica.

L'informativa di cui all'Allegato B sarà resa a tutti coloro che saranno coinvolti nell'indagine successiva alla segnalazione.

In ogni caso, all'esito di tale verifica:

- nel caso di infondatezza, il RSIS comunica al segnalante (attraverso la stessa modalità di ricezione della segnalazione) l'esito motivato e la conclusione del procedimento;
- qualora dall'esito della verifica, la segnalazione risulti fondata, il RSIS procede a informare (i) il segnalante circa l'esito positivo delle indagini, (ii) il segnalato tramite comunicazione separata, (iii) il Collegio Sindacale tramite apposita comunicazione.

Nel corso del processo di analisi della segnalazione, il RSIS effettua la valutazione della segnalazione in termini di rilevanza e gravità della stessa e procede ad informare il segnalante (attraverso la stessa modalità di ricezione della segnalazione) e il segnalato (tramite comunicazione separata) circa gli esiti della valutazione stessa. Nel caso in cui si siano verificate violazioni gravi, il RSIS informa tempestivamente il Consiglio di Amministrazione ed il Collegio Sindacale affinché valutino l'eventuale adozione di provvedimenti decisionali e disciplinari di rispettiva competenza.

In qualunque fase del procedimento – e senza attendere l'esito della valutazione – il RSIS riferisce direttamente e senza indugio le informazioni rilevanti oggetto della segnalazione agli Organi Aziendali che provvedono ad adottare i relativi provvedimenti, anche d'urgenza, ove risulti necessario, ivi incluso, se del caso, informativa al Responsabile della Funzione Antiriciclaggio qualora ricorrano i presupposti per la predisposizione di una segnalazione di operazione sospetta. Qualora oggetto della segnalazione sia il medesimo RSIS e la segnalazione venga ritenuta fondata e rilevante, l'informativa tempestiva agli Organi Aziendali dovrà essere fornita direttamente dalla Funzione di riserva.

Nel caso in cui il segnalante sia corresponsabile della violazione oggetto di segnalazione, la Società può prevedere un trattamento privilegiato nei suoi confronti rispetto agli altri corresponsabili, salvi i casi in cui la condotta del segnalante risulti di particolare gravità.

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 SGR. In ogni caso, la procedura deve concludersi entro 2 mesi dalla ricezione della segnalazione, salvo casi eccezionali e opportunamente motivati in cui l'esame e la valutazione della segnalazione possa estendersi fino a 3 mesi, previa comunicazione al Collegio Sindacale.

7. FORME DI TUTELA DEL SEGNALANTE

7.1 Tutela dell'anonimato

Al fine di evitare che il timore di subire conseguenze pregiudizievoli possa indurre a non segnalare le violazioni, l'identità del segnalante non può essere rivelata, salvo il suo espresso e libero consenso, e tutti coloro che sono coinvolti nella gestione della segnalazione, 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'articolo 2043 del Codice Civile, nonché le ipotesi in cui l'anonimato non sia opponibile per legge.

L'anonimato del segnalante è altresì garantito nell'ambito del procedimento disciplinare quando la contestazione al segnalato sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. L'identità del segnalante può invece essere rivelata al soggetto segnalato, con il consenso del segnalante, ovvero quando la contestazione sia basata principalmente sulla segnalazione e pertanto la conoscenza dell'identità è assolutamente indispensabile per la difesa del segnalato.

Le violazioni dell'obbligo di riservatezza, inclusa la divulgazione di informazioni in base a cui l'identità del segnalante 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.

7.2 Divieto di discriminazione

Il personale che effettua una segnalazione ai sensi della presente *policy* non può essere sanzionato, licenziato (salvo i casi di corresponsabilità accertata) o sottoposto ad alcuna misura discriminatoria avente effetti sulle condizioni di lavoro per motivi collegati alla segnalazione (fermo restando quanto previsto nel successivo Paragrafo 8). Il licenziamento ritorsivo o discriminatorio del segnalante è nullo e sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del Codice Civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. Per misure discriminatorie si intendono le azioni disciplinari ingiustificate, anche solo tentate o minacciate, le molestie sul luogo di lavoro ed ogni altra forma di ritorsione che provoca o può provocare alla persona segnalante o alla persona che ha sporto denuncia, in via diretta o indiretta, un danno ingiusto.

È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, a demansionamenti, licenziamenti, trasferimenti o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure siano fondate su ragioni estranee alla segnalazione stessa.

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'Ispettorato Nazionale del Lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Nei casi più gravi, e qualora sia possibile, la SGR può valutare di disporre il trasferimento per incompatibilità ambientale del segnalante, previo consenso del medesimo.

Il personale che ritiene di aver subito una discriminazione ne dà notizia circostanziata al RSIS che, accertata la fondatezza, segnala la casistica agli Organi Aziendali competenti, affinché siano adottati i provvedimenti necessari a ripristinare la situazione e/o rimediare agli effetti negativi della discriminazione.

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

Le medesime misure di protezione si applicano anche:

- al facilitatore;
- alle persone del medesimo contesto lavorativo della persona segnalante e che sono legate ad essa da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro della persona segnalante, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- agli enti di proprietà della persona segnalante o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone;
- in caso di segnalazione anonima, se la persona segnalante è stata successivamente identificata.

8. RESPONSABILITÀ DEL SEGNALANTE

La presente *Policy* lascia impregiudicata la responsabilità penale e disciplinare del segnalante, nell'ipotesi di segnalazione calunniosa e diffamatoria ai sensi del Codice Penale o ai sensi dell'articolo 2043 del Codice Civile.

Fatte salve le specifiche limitazioni di responsabilità previste dall'art. 20 del D.lgs. 24/2023, sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente *Policy*, quali le segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il segnalato e/o altri soggetti, ed ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente *Policy*.

9. PROTEZIONE DEI DATI E ARCHIVIAZIONE DEI DOCUMENTI

Al fine di assicurare la ricostruzione delle diverse fasi del processo di segnalazione, è cura del RSIS (ovvero della Funzione di Riserva, per le segnalazioni a lui pervenute) 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);
- 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.

Le funzioni competenti archiviano la documentazione inerente al processo sanzionatorio e disciplinare.

È tutelato, ai sensi della normativa vigente e delle procedure aziendali in materia di privacy, il trattamento dei dati personali delle persone coinvolte e/o citate nelle segnalazioni.

10. AGGIORNAMENTO DELLA POLICY

La SGR sottopone a verifica l'intero contenuto della presente *policy* ogni qualvolta si verifichi un cambiamento rilevante nell'operatività della Società ovvero nel sistema di segnalazione delle violazioni. La revisione e l'aggiornamento della presente *policy* viene effettuata dalla Funzione *Compliance* e sottoposta all'approvazione dei competenti organi aziendali.

ALLEGATO A – Modulo per la segnalazione interna delle violazioni

Nome e Cognome del segnalante	
Inquadramento e qualifica professionale	
Sede di lavoro	
Recapiti	
Luogo in cui si è verificato il fatto	
Descrizione dei fatti oggetto di segnalazione	
Nome/i e cognome/i del/dei soggetto/i segnalato/i	
Nome/i e cognome/i del/dei soggetto/i a conoscenza dei fatti oggetto di segnalazione (eventuale)	
Ulteriori informazioni che possano fornire utile riscontro circa la sussistenza dei fatti oggetto di segnalazione (eventuale)	
Allegati pertinenti (eventuale)	

ALLEGATO B – Informativa per il dipendente soggetto a investigazione interna

[Data], [Luogo]

Oggetto: informativa *privacy* per la realizzazione di un'investigazione interna

Gentile [...]

Nell'ambito di una indagine relativa a [*descrizione sommaria del caso*], la Società ha necessità di svolgere accertamenti ed esaminare e – se opportuno – estrarre copia di [*indicare oggetto indagine*].

La Società intende procedere a un esame complessivo del materiale raccolto al fine di valutare [*indicare la finalità dell'indagine*] per la difesa dei propri diritti. Il titolare del trattamento dei dati raccolti con l'indagine è la Società. I suoi dati saranno utilizzati solamente per le finalità menzionate e potranno essere trattati con o senza ausilio di mezzi elettronici o automatizzati. I soggetti che prenderanno visione dei suoi dati sono l'Organismo di Vigilanza della Società, nonché l'Amministratore Delegato della Società e/o coloro sono incaricati da quest'ultimo di seguire l'eventuale procedimento giudiziario che potrebbe derivarne. Il conferimento dei suoi dati non necessita del suo consenso in quanto i dati sono raccolti al fine della tutela dei diritti della Società. Un suo eventuale rifiuto sarebbe illegittimo e in tal caso la Società si troverebbe costretta ad adottare le misure più opportune per il conseguimento delle finalità indicate e potrebbe dare luogo a conseguenze anche sul piano disciplinare. I dati potranno essere condivisi con consulenti esterni della Società, esclusivamente per le finalità sopra indicate. I dati e le informazioni saranno conservati per il tempo strettamente necessario alla conduzione delle verifiche e alla eventuale tutela del diritto di difesa della Società, oltre che per l'eventuale ulteriore periodo durante il quale sussista un interesse legittimo alla conservazione delle informazioni e dei dati stessi, tra cui l'interesse alla difesa in sede giudiziaria; dopodiché saranno cancellati o resi anonimi. Lei ha i diritti previsti dagli artt. 15 e ss. GDPR. Per l'esercizio dei suoi diritti può rivolgersi tramite comunicazione scritta o via e-mail scrivendo a [...].

Le ricordiamo che qualora ritenga il trattamento dei dati personali illecito può proporre reclamo al Garante per la Protezione dei Dati Personali.

La ringraziamo sin d'ora per la collaborazione e le inviamo cordiali saluti.