

## **POLICY WHISTLEBLOWING**

### **Copernico SIM S.p.A.**

Approvata dal Cda il 23 aprile 2020	
1° aggiornamento del 28 marzo 2024	
2° aggiornamento del 24 giugno 2026	Introduzione dell'informativa prevista al segnalante e al segnalato, l'obbligo per il soggetto segnalante di dichiarare se vi è un interesse privato collegato alla segnalazione, l'impegno ad adottare un trattamento privilegiato per il segnalante corresponsabile delle violazioni.

## SOMMARIO

PREMESSA.....	5
RIFERIMENTI NORMATIVI .....	5
DEFINIZIONI .....	6
1. OGGETTO E CONTENUTO DELLE SEGNALAZIONI .....	8
1.1. Oggetto delle segnalazioni.....	8
1.2. Esclusioni .....	8
1.3. Segnalazioni anonime.....	8
2. SOGGETTI LEGITTIMATI AD EFFETTUARE SEGNALAZIONI.....	8
3. CANALI DI SEGNALAZIONE.....	9
3.1. Segnalazione interna.....	9
3.1.1. Segnalazione interna tramite canali diversi.....	9
3.2. Presidi per la riservatezza e protezione dei dati .....	9
3.2.1. Gestione tramite la piattaforma dedicata .....	10
3.2.2. Colloquio personale .....	10
3.3. Responsabili whistleblowing .....	10
3.4. Canale di Segnalazione Esterna .....	11
3.4.1. ANAC.....	11
3.4.2. Divulgazione pubblica .....	11
3.4.3. Denuncia All’Autorità giudiziaria.....	11
3.4.4. Segnalazione alla SIM d’Italia .....	11
3.5. Pubblicità.....	12

4.	GESTIONE DELLA SEGNALAZIONE.....	12
4.1.	Obblighi di riscontro nei confronti del segnalante .....	12
4.2.	Trattamento della segnalazione .....	12
4.2.1.	Istruttoria .....	12
4.2.2.	Segnalazione fondata .....	12
4.2.3.	Segnalazione infondata .....	13
4.3.	Modalità di custodia della documentazione .....	13
4.4.	Tempi di conservazione della documentazione .....	13
5.	TUTELE.....	13
5.1.	Soggetti tutelati .....	13
5.2.	Condizioni per la protezione .....	14
5.3.	Riservatezza .....	14
5.3.1.	Eccezione .....	14
5.4.	Trattamento privilegiato in caso di corresponsabilità .....	14
5.5.	Divieto di ritorsioni .....	14

## PREMESSA

Copernico SIM (d'ora innanzi anche la "SIM" o la "Società" promuove una cultura aziendale improntata alla legalità, caratterizzata da comportamenti corretti e fondati su dignità e rispetto consapevole.

La presente "Policy Whistleblowing" (a seguire, la "policy" o, anche solo, il "documento") si propone di delineare il processo di gestione della segnalazione di comportamenti illegittimi – identificando altresì i canali di comunicazione che ne consentono la ricezione, l'analisi e il trattamento da parte della funzione aziendale deputata – finalizzato allo svolgimento delle opportune verifiche e all'adozione dei rimedi necessari per evitarne la reiterazione nel tempo, avendo cura di proteggere le persone che segnalano le eventuali violazioni della normativa, nazionale ed europea, che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui sono venute a conoscenza in un contesto lavorativo pubblico o privato.

Il documento è parte integrante del sistema dei controlli interni ed ha lo scopo di fornire ai dipendenti e ai collaboratori della SIM, che abbiano il ragionevole sospetto che si sia verificato o si possa verificare un comportamento illegittimo all'interno della stessa, uno strumento per segnalarlo secondo modalità che garantiscano la riservatezza della segnalazione, del soggetto segnalante e del soggetto segnalato.

Il documento è sottoposto a periodica revisione

## RIFERIMENTI NORMATIVI

I principali riferimenti normativi in materia di segnalazione di comportamenti illegittimi sono i seguenti:

- D. lgs. n. 395/1993 ("TUB"), art. 52-bis<sup>1</sup>;
- D. lgs. n. 58/1998 ("TUF"), art. 4-undecies<sup>2</sup>;
- Circ. n. 285/2013 di SIMd'Italia (cd. "Disposizioni di vigilanza");
- D. lgs. n. 24/2023, attuativo della Direttiva UE 2019/1937;
- Regolamento (UE) 2016/679 ("GDPR").

## DEFINIZIONI

### *Segnalazione*

Qualsiasi comunicazione scritta, orale o esposta in un colloquio, anche in forma anonima, contenente informazioni sulle violazioni.

### *Violazioni*

Condotte illecite rilevanti quali reato presupposto ai sensi del D. lgs. n. 231/2001 o relative a violazioni del “Modello di organizzazione e gestione” (laddove adottato dalla SIM).

### *Illeciti*

Illeciti che rientrano nell’ambito di applicazione degli atti dell’Unione Europea o nazionali rilevanti, relativi ad appalti pubblici, servizi, prodotti e mercati finanziari, prevenzione del riciclaggio, sicurezza e conformità dei prodotti, sicurezza dei trasporti, tutela dell’ambiente, sicurezza degli alimenti e dei mangimi, salute e benessere degli animali, salute pubblica, protezione dei consumatori, tutela della vita e protezione dei dati personali, sicurezza delle reti e dei sistemi informativi. Si considerano tali anche le violazioni che ledono gli interessi finanziari dell’Unione Europea, le violazioni di norme in materia di concorrenza e aiuti di Stato e le violazioni di norme in materia tributaria.

### *Informazioni*

Tutte le informazioni, inclusi sospetti fondati, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell’organizzazione con cui la persona segnalante o colui che sporge denuncia all’autorità giudiziaria/contabile intrattiene un rapporto giuridico; o riguardanti condotte volte ad occultare tali violazioni.

### *Segnalazione interna*

La segnalazione effettuata attraverso il canale interno di segnalazione.

### *Segnalazione esterna*

La segnalazione effettuata tramite il canale di segnalazione esterna gestito da ANAC o altri canali alternativi, in quanto consentiti<sup>3</sup>.

### *Divulgazione pubblica*

La diffusione di informazioni sulle violazioni tramite la stampa ovvero mezzi elettronici o comunque tramite mezzi di informazione in grado di raggiungere un numero elevato di persone.

### *Segnalante (whistleblower)*

La persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell’ambito del proprio contesto lavorativo.

### *Facilitatore*

La persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno dello stesso contesto lavorativo e la cui assistenza deve essere mantenuta riservata.

## 1. OGGETTO E CONTENUTO DELLE SEGNALAZIONI

### 1.1. Oggetto delle segnalazioni

Ai sensi della presente policy, possono essere oggetto di segnalazioni le circostanze di cui il segnalante sia venuto a conoscenza nel contesto lavorativo, che riguardino:

- illeciti amministrativi, contabili, civili o penali secondo la normativa nazionale;
- illeciti rilevanti ai sensi della normativa sulla responsabilità amministrativa degli enti ex D. lgs. n. 231/2001 (cd. reati presupposto) e violazioni del cd. Modello 231 (ove presente);
- violazione di norme e atti dell'Unione Europea consistenti in:
  - illeciti rilevanti ai sensi della normativa dell'Unione Europea riguardanti, tra l'altro, i seguenti settori: servizi, prodotti e mercati finanziari; prevenzione del riciclaggio e del finanziamento del terrorismo; protezione dei dati personali; sicurezza delle reti e dei sistemi informativi;
  - atti o omissioni che ledono gli interessi finanziari dell'Unione Europea;
  - atti o omissioni riguardanti il mercato interno, incluse quelle relative a concorrenza, aiuti di Stato e alla normativa in materia fiscale;
  - atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni negli ambiti sopra riportati.

La segnalazione deve contenere tutte le informazioni utili che consentano al responsabile della gestione delle segnalazioni di accertare la fondatezza di quanto segnalato e di attivare pertanto la relativa istruttoria. È quindi opportuno che il segnalante alleghi documenti che possano riscontrare la segnalazione e il riferimento ad altre persone che possano fornire ulteriori informazioni o corroborare il contenuto della segnalazione.

In particolare, la segnalazione deve riportare in modo chiaro le seguenti informazioni:

- le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- la descrizione del fatto;
- il nome e il cognome, oppure ogni altra informazione utile a identificare l'autore del fatto;
- le generalità di eventuali altri soggetti coinvolti o che possono riferire sul fatto.

Le informazioni devono essere veritiere. Pertanto, non si considerano pertinenti le semplici supposizioni o le notizie di pubblico dominio, mentre assumono rilevanza i fondati sospetti.

### 1.2. Esclusioni

Le segnalazioni non devono riguardare contestazioni, rivendicazioni o richieste legate a un interesse di carattere personale del segnalante, incluso quanto relativo al rapporto di lavoro di quest'ultimo. Il segnalante è tenuto, quindi, a precisare se ha un interesse personale nella vicenda, oltre a descrivere i fatti. Nel caso in cui il segnalante esegua la segnalazione tramite piattaforma dedicata (vedi il punto 3.2.1), sarà possibile compilare una sezione che specifica se lo stesso è titolare di un interesse personale.

### 1.3. Segnalazioni anonime

Le segnalazioni anonime, ove adeguatamente circostanziate, sono regolarmente gestite nell'ambito

della presente policy, con ogni relativa tutela del segnalante, laddove successivamente identificato.

## 2. SOGGETTI LEGITTIMATI AD EFFETTUARE SEGNALAZIONI

Con riferimento alla SIM e ai soggetti ad essa legati da rapporti contrattuali, sono legittimati ad effettuare la segnalazione:

- i lavoratori subordinati (anche prima dell'assunzione, se le informazioni sulle violazioni vengono acquisite durante la fase di selezione e anche successivamente alla cessazione del rapporto, purché le informazioni siano state acquisite in costanza di rapporto o nella fase di selezione);
- i lavoratori autonomi e i collaboratori, ivi inclusi consulenti Finanziari abilitati all'offerta fuori sede della Società;
- i liberi professionisti e i consulenti;
- i volontari e tirocinanti, retribuiti e non retribuiti;
- i titolati di quote o azioni;
- le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto;
- membri del Consiglio di Amministrazione e membri del Collegio Sindacale.

## 3. CANALI DI SEGNALAZIONE

### 3.1. Segnalazione interna

La SIM ha istituito i seguenti canali di segnalazione interna:

- in forma scritta, riservata o completamente anonima, attraverso il canale informatico dedicato (cd. "piattaforma"), accessibile tramite appositi link presenti nell'app dedicata al personale e nel sito internet della Società.

La piattaforma fornisce al segnalante un codice alfanumerico con il quale egli può tenere traccia dello stato di lavorazione della segnalazione effettuata, nonché interagire con il responsabile whistleblowing, attraverso lo strumento di messaggistica presente nella piattaforma.

Qualunque sia la forma di comunicazione attivata, il segnalante deve specificare che si tratta di una segnalazione per la quale si intende mantenere riservata la propria identità e beneficiare delle tutele previste dalla normativa nel caso di ritorsioni.

Tramite la piattaforma, il segnalante può altresì richiedere un incontro diretto con il responsabile whistleblowing.

#### 3.1.1. Segnalazione interna tramite canali diversi

Qualora la segnalazione giunga per canali diversi da quelli sopra indicati, essa dovrà essere trasmessa dal soggetto ricevente, direttamente e senza indugio, al responsabile whistleblowing, avendo cura di informare contestualmente il segnalante. Il ricevente deve effettuare tale trasmissione nel rispetto di criteri di massima riservatezza e con modalità idonee a tutelare sia l'identità del segnalante, sia la riservatezza del contenuto della segnalazione, inclusi i riferimenti ai soggetti coinvolti. Se in forma cartacea, dev'essere trasmesso l'originale del documento contenente la segnalazione, inclusi gli eventuali allegati, senza che ne venga fatta nessuna copia. Eventuali comunicazioni ricevute in via

elettronica dovranno essere trasmesse con modalità sicure e tali da mantenere evidenza dell'intero processo di trasmissione adottato, avendo cura di cancellare ogni traccia della segnalazione dai propri sistemi/archivi informatici.

Qualora la segnalazione riguardi specifici soggetti, la segnalazione, anziché essere inviata al Responsabile dei sistemi interni di segnalazione, deve essere trasmessa:

- Al Presidente del Collegio Sindacale, nel caso di segnalazioni riguardanti:
  - il Responsabile dei sistemi interni di segnalazione

### 3.2. Presidi per la riservatezza e protezione dei dati

Attraverso i presidi descritti nel presente paragrafo è garantita la riservatezza dell'identità del segnalante, delle

persone coinvolte o menzionate nella segnalazione, del facilitatore, del contenuto della segnalazione e della relativa documentazione di supporto.

#### 3.2.1. Gestione tramite la piattaforma dedicata

Conformemente a quanto richiesto dall'art. 32 del GDPR, la piattaforma:

- permette di impostare e modulare l'accesso alle informazioni, in base alle diverse esigenze e abilitazioni. A tal fine sono definiti appositi diritti di accesso e di trattamento dei dati (in base alle autorizzazioni) e necessità operative (attraverso credenziali personali);
- prevede un sistema di cifratura che impedisce una correlazione diretta tra il segnalante e la segnalazione. Tutte le informazioni che possono rivelare i contenuti di una segnalazione e l'identità del suo autore, o che possono dare indicazioni sull'attività di un segnalante, sono infatti protette e cifrate su più livelli;
- è installata su una infrastruttura di server dedicati che garantiscono la necessaria resistenza ad attacchi informatici in base allo stato dell'arte;
- registra attraverso un sistema di Log management, in modo anonimo e criptato, tutte le operazioni ivi svolte;
- può essere reinstallata, completa degli ultimi set di dati disponibili, su diversi server disponibili, in caso di disaster recovery.

Ai sensi dell'art. 5 del GDPR, il trattamento dei dati personali, quale effettuato attraverso la piattaforma dedicata, risulta proporzionale e necessario alle finalità di segnalazione perseguite, permettendo un accesso sicuro dovuto alla separazione del processo di iscrizione e del processo di segnalazione.

La piattaforma consente – a personale autorizzato – la raccolta e il trattamento esclusivamente dei dati necessari alla gestione del processo di segnalazione; tali dati sono conservati per il tempo strettamente necessario al raggiungimento delle finalità per le quali vengono raccolti. La piattaforma garantisce l'esattezza dei dati trattati, i quali permettono l'identificazione univoca del segnalante attraverso l'assegnazione di una chiave di cifratura accessibile solo dai soggetti autorizzati alla ricezione delle segnalazioni.

#### 3.2.2. Colloquio personale

Ove richiesto, l'incontro tra il segnalante e il responsabile whistleblowing deve avvenire con modalità riservate. Laddove la relazione tra tali soggetti non risulti usuale nell'ambito del normale rapporto lavorativo, l'incontro dovrà avvenire al di fuori della sede della SIM.

### 3.3. Responsabili whistleblowing

Il Consiglio di Amministrazione ha nominato quale **Responsabile dei sistemi interni di segnalazione** il **Responsabile della Funzione Compliance e Antiriciclaggio**, il quale assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio al Consiglio di Amministrazione e al Collegio Sindacale le informazioni oggetto di segnalazione, qualora la violazione sia stata accertata.

Il Responsabile dei sistemi interni di segnalazione, in linea con il principio di proporzionalità, gestisce direttamente le fasi di ricezione, esame e valutazione del procedimento di segnalazione.

La gestione del canale di segnalazione interna è affidata al responsabile della funzione di conformità alle norme ("responsabile whistleblowing"). In caso di suo impedimento, tale onere è ricondotto al Responsabile della Funzione di revisione interna.

Qualora la segnalazione riguardi il Responsabile dei sistemi interni di violazione, la segnalazione verrà inviata al Presidente del Collegio Sindacale, come indicato al paragrafo 3.1.1.

I soggetti sopra indicati, preposti alla ricezione, all'esame e alla valutazione delle segnalazioni, non partecipano all'adozione degli eventuali provvedimenti decisionali, che sono rimessi alle funzioni o agli organi aziendali competenti.

### 3.4. Canale di Segnalazione Esterna

#### 3.4.1. ANAC

Il segnalante può utilizzare il canale di segnalazione esterno attivato dall'ANAC, accessibile dal sito web di tale autorità ([www.anticorruzione.it](http://www.anticorruzione.it)).

Il ricorso a tale canale è attivabile esclusivamente al verificarsi di una delle seguenti condizioni:

- la segnalazione effettuata dal segnalante tramite il canale di segnalazione interna non ha avuto seguito;
- il segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, questa non avrebbe idoneo seguito o potrebbe determinare il rischio di ritorsione;
- il segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

#### 3.4.2. Divulgazione pubblica

Il segnalante può rendere di pubblico dominio le informazioni relative alle violazioni. A tal fine, egli può utilizzare gli organi di stampa, i mezzi elettronici ovvero i mezzi di diffusione in grado di raggiungere un elevato numero di persone.

Il ricorso da parte del segnalante alla divulgazione pubblica comporta le tutele previste dalla presente policy solo al verificarsi di una delle seguenti condizioni:

- il segnalante ha previamente effettuato una segnalazione interna ed esterna, oppure ha effettuato

direttamente una segnalazione esterna (sussistendone i presupposti), senza aver ricevuto riscontro nei termini previsti dalla legge;

- il segnalante ha fondato motivo di ritenere che la violazione possa rappresentare un pericolo imminente o palese per il pubblico interesse;
- il segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni oppure possa non avere efficace seguito, tenuto conto delle particolari circostanze del fatto segnalato (per es., a causa del rischio concreto di occultamento o di distruzione delle prove).

#### 3.4.3. Denuncia all'Autorità giudiziaria

Il segnalante può rivolgersi anche all'Autorità giudiziaria, presentando una denuncia di condotte illecite di cui sia venuto a conoscenza nel contesto lavorativo, conservando le tutele previste dalla presente procedura, per quanto di competenza della SIM.

#### 3.4.4. Segnalazione alla Banca d'Italia

Per denunciare eventuali violazioni della normativa o presunte anomalie gestionali, che abbia riscontrato presso Copernico Sim Spa, il segnalante può infine rivolgersi alla Banca d'Italia (istruzioni al link:

<https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/index.html>).

#### 3.5. Pubblicità

La SIM mette a disposizione del pubblico informazioni chiare sul canale di segnalazione attivato, sulle procedure da seguire e sui presupposti necessari per poter effettuare le segnalazioni, sia interne che esterne.

La Policy è consultabile all'interno dell'intranet aziendale per il personale dipendente e, comunque, è pubblicata in una sezione dedicata del sito web aziendale, dalla quale è pure accessibile la piattaforma.

### 4. GESTIONE DELLA SEGNALAZIONE

#### 4.1. Obblighi di riscontro nei confronti del segnalante

Il responsabile whistleblowing rilascia al segnalante un avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione (purché possibile, in quanto la segnalazione non è giunta in forma anonima e con mezzi diversi dalla piattaforma dedicata) Il segnalante, inoltre, sarà informato sull'evoluzione e sull'esito delle considerazioni e valutazioni eseguite circa la segnalazione – se la segnalazione è avvenuta tramite piattaforma, alla modifica dello status della segnalazione eseguita dal responsabile, il sistema invierà al segnalante gli aggiornamenti; se la segnalazione è pervenuta tramite altri canali, il responsabile avrà cura di comunicare al segnalante tramite e-mail, PEC o lettera raccomandata gli sviluppi dell'analisi e l'esito della segnalazione.

## 4.2. Trattamento della segnalazione

Il responsabile whistleblowing provvede alle seguenti attività:

- a) valutazione preliminare del contenuto della segnalazione, al fine di verificare la presenza dei presupposti necessari all'avvio dell'istruttoria ovvero procedere alla relativa archiviazione;
- b) svolgimento dell'istruttoria, finalizzata ad accertare la fondatezza della segnalazione. L'istruttoria è effettuata assicurando un diligente e corretto seguito alle segnalazioni, con ragionevole tempestività e conducendo le verifiche in maniera equa, imparziale e accurata.
- c) La Società informa il soggetto segnalato (tramite e-mail, PEC o lettera raccomandata, a discrezione della valutazione del Responsabile Whistleblowing) circa i fatti a lui contestati e i suoi diritti (es. accesso ai dati, nei limiti della legge). L'informativa al segnalato può essere differita qualora vi sia il rischio concreto che la comunicazione possa pregiudicare l'integrità delle indagini o l'accertamento dei fatti (es. rischio di inquinamento delle prove).

### 4.2.1. Istruttoria

Nello svolgimento dell'istruttoria, il responsabile whistleblowing può:

- chiedere al segnalante chiarimenti e ulteriori informazioni o integrazioni, anche documentali, in merito alla segnalazione presentata;
- avvalersi, nel rispetto delle tutele previste dalla presente policy, della collaborazione di altri soggetti presenti all'interno della SIM (purché non coinvolti nella segnalazione) nonché, con costi a carico della SIM, di consulenti esterni.

Nel corso dell'istruttoria, il responsabile whistleblowing fornisce informativa al segnalante in merito allo stato di avanzamento della stessa, entro 3 mesi dalla data dell'avviso del relativo ricevimento, e comunque entro 3 mesi e 7 giorni dalla ricezione della segnalazione, tramite i canali indicati al punto 4.1.

Alla conclusione dell'istruttoria, il responsabile whistleblowing redige una relazione documentata che riporta la descrizione della segnalazione, le modalità di svolgimento dell'istruttoria, gli elementi raccolti, le conclusioni tratte e un piano per l'adozione delle azioni correttive.

### 4.2.2. Segnalazione fondata

Nel caso in cui la segnalazione sia ritenuta fondata, il responsabile whistleblowing comunica l'esito al presidente del Consiglio di Amministrazione. Laddove la segnalazione riguardi quest'ultimo, la comunicazione è inviata al presidente del Collegio Sindacale. Al riguardo, il responsabile whistleblowing provvederà – anche in relazione ai profili di illiceità riscontrati – a presentare denuncia all'Autorità giudiziaria competente.

### 4.2.3. Segnalazione infondata

Laddove la segnalazione sia ritenuta una mera lamentela (perché relativa a eventi già segnalati e/o conosciuti ovvero in quanto non rientri nel campo di applicazione della normativa in materia di whistleblowing), il responsabile whistleblowing comunica tale esito al segnalante (purché si tratti di

segnalazione non anonima) e al presidente del Consiglio di Amministrazione.

Si considera infine una segnalazione in mala fede la comunicazione effettuata al solo scopo di danneggiare o arrecare pregiudizio alle persone coinvolte. In tal caso, il responsabile whistleblowing comunica l'esito dell'istruttoria al presidente del Consiglio di Amministrazione e al segnalante, ribadendo a quest'ultimo che non potranno essere riconosciute le tutele altrimenti previste dalla disciplina di riferimento (la SIM potrà infatti avviare un'azione legale/disciplinare verso il segnalante, sussistendo le condizioni di cui al successivo paragrafo 5.2).

La società applicherà sanzioni disciplinari nei confronti dei soggetti segnalanti dipendenti o collaboratori per i quali è stato accertato dolo o colpa grave, segnalazioni false e/o infondate al solo scopo di diffamazione, calunnia o danno al segnalato o agli altri soggetti citati nella segnalazione.

#### 4.3. Modalità di custodia della documentazione

Tutta la documentazione è gestita, per quanto possibile, tramite la piattaforma dedicata. Nei casi in cui ciò non sia possibile (ricezione di documentazione per vie diverse dalla piattaforma), essa è custodita in armadi chiusi a chiave e non identificabili dall'esterno.

#### 4.4. Tempi di conservazione della documentazione

La documentazione raccolta è conservata per il tempo strettamente necessario alla gestione della segnalazione e comunque non oltre cinque anni a decorrere dalla data di comunicazione della conclusione dell'Istruttoria.

### 5. TUTELE

#### 5.1. Soggetti tutelati

Le tutele previste dalla disciplina vigente e recepite dalla presente policy si applicano ai seguenti soggetti:

- segnalante;
- facilitatore;
- persone dello stesso contesto lavorativo del segnalante, incluso chi ha sporto una denuncia all'Autorità giudiziaria o contabile ovvero ha effettuato una divulgazione pubblica, e che è legato a esso da uno stabile legame affettivo o di parentela entro il quarto grado;
- colleghi di lavoro del segnalante, incluso chi ha sporto una denuncia all'Autorità giudiziaria o contabile ovvero ha effettuato una divulgazione pubblica, che lavorano nello stesso contesto lavorativo e che hanno con detta persona un rapporto abituale e corrente;
- enti di proprietà del segnalante, incluso chi ha sporto una denuncia all'Autorità giudiziaria o contabile o ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, e agli enti che operano nello stesso contesto lavorativo di tali soggetti.

#### 5.2. Condizioni per la protezione

Le tutele si applicano a condizione che, al momento della segnalazione o della denuncia all’Autorità giudiziaria o della divulgazione pubblica, il segnalante avesse fondato motivo di ritenere che le informazioni sulle violazioni fossero vere e rientrassero nell’ambito di applicazione del D. lgs. n. 24/2023 e fossero state comunicate con le modalità e nei termini previsti dallo stesso.

Fermo quanto previsto per le segnalazioni in mala fede, non incidono sulle tutele i motivi che hanno portato il segnalante ad effettuare la segnalazione.

### 5.3. Riservatezza

L’identità del segnalante e qualsiasi altra informazione da cui possa trarsi, anche indirettamente, tale identità non possono essere rivelate, senza il consenso espresso del segnalante medesimo, a persone diverse da quelle competenti a ricevere o a gestire le segnalazioni.

Le medesime tutele sono garantite, con riferimento all’identità delle persone coinvolte e delle persone menzionate nella segnalazione, fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore del segnalante.

Nell’ambito del procedimento disciplinare verso le persone coinvolte, l’identità del 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.

#### 5.3.1. Eccezione

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

### 5.4. Trattamento Privilegiato in caso di Corresponsabilità

In conformità alle Disposizioni di Vigilanza di Banca d’Italia, la Società prevede un **trattamento privilegiato** per il segnalante che risulti co-responsabile delle violazioni segnalate, a condizione che:

1. La segnalazione sia fornita **tempestivamente** e prima che l’ente abbia altrimenti avuto notizia dell’illecito.
2. Il contributo del segnalante sia determinante per l’accertamento della violazione e l’identificazione degli altri responsabili.
3. Il segnalante collabori attivamente e in buona fede per tutta la durata dell’istruttoria.

In tali casi, la Società si impegna a valutare l’applicazione di **attenuanti nelle sanzioni disciplinari** previste dal sistema sanzionatorio aziendale, compatibilmente con il quadro normativo vigente e senza pregiudizio per eventuali responsabilità civili o penali

### 5.5. Divieto di ritorsioni

La SIM assicura ai soggetti tutelati di cui al paragrafo 5.1 la protezione contro le ritorsioni, sia effettive che tentate o minacciate. Per ritorsione s’intende qualunque comportamento, anche

omissivo, motivato dalla segnalazione e atto a provocare, direttamente o indirettamente, al soggetto tutelato un danno ingiusto o comunque un evento pregiudizievole.

A mero titolo esemplificativo, possono considerarsi ritorsioni i seguenti comportamenti:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di mansioni o la modifica dell’orario di lavoro;
- le referenze negative;
- le azioni disciplinari o altra sanzione, anche pecuniaria;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- la lesione della reputazione, anche sui social media;
- l'annullamento di una licenza o di un permesso.

Sono nulli gli atti che costituiscono ritorsioni e i loro autori sono passibili di azioni giudiziarie e disciplinari.

Il segnalante che ritenga di aver subito ritorsioni può rivolgersi all’ANAC.

## **RELAZIONE ANNUALE SULLE SEGNALAZIONE RICEVUTE**

Il responsabile dei sistemi interni di segnalazione redige una relazione annuale sul corretto funzionamento dei sistemi interni di segnalazione, contenente le informazioni aggregate sulle risultanze dell’attività svolta a seguito delle segnalazioni ricevute; la relazione è approvata dagli organi aziendali e messa a disposizione del personale.

Nel dettaglio, la Relazione annuale contiene i seguenti contenuti minimi:

- analisi di tutte le segnalazioni (ricevute/archivate/valutate), le tipologie di violazioni segnalate maggiormente, e gli esiti degli approfondimenti condotti (segnalazioni accolte/ respinte);
- metodologia utilizzata per le valutazioni effettuate, evidenze emerse (eventuali provvedimenti disciplinari e/o sanzioni) ed eventuali interventi correttivi sul processo in oggetto.

La Relazione deve essere predisposta anche nel caso di mancata ricezione di segnalazioni.