

## Manuale delle Procedure Interne

### Policy Whistleblowing

Proposto da: Direttore Generale	14/12/2023
Approvato da: Consiglio di Amministrazione	14/12/2023

**Replica SIM S.p.A.**

Sede legale Corso Sempione, 2  
20154 Milano - replica@legalmail.it

[replicasim.com](http://replicasim.com)

P. IVA - C.Fisc. Reg. Imprese 11064390963  
R.E.A. 2576681 Capitale sociale 10.500.000,00 €

## INDICE

1. PREMESSA.....	3
2. OBIETTIVI .....	5
3. DEFINIZIONI.....	6
4. SOGGETTI SEGNALANTI.....	7
5. CANALE PER LE SEGNALAZIONI INTERNE .....	7
6. CARATTERISTICHE DELLE VIOLAZIONI E DELLE SEGNALAZIONI.....	8
7. PORTALE WHISTLEBLOWING.....	9
8. MODALITÀ DI TRASMISSIONE DELLE SEGNALAZIONI.....	10
9. GESTIONE DELLE SEGNALAZIONI.....	10
10. TUTELA E RESPONSABILITÀ DEL SEGNALANTE.....	13
11. ESTENSIONE DELLA TUTELA DEL SEGNALANTE AD ALTRI SOGGETTI .....	15
12. TUTELA DEL SEGNALATO.....	15
13. REPORTISTICA .....	16
14. CONSERVAZIONE DELLA DOCUMENTAZIONE .....	16
15. PROTEZIONE DEI DATI PERSONALI.....	16
16. ONERI DI PUBBLICITÀ PER REPLICA SIM A FINI DI TRASPARENZA DEL WHISTLEBLOWING.....	17
17. IL CANALE DI SEGNALAZIONE ESTERNA ALL'AUTORITÀ DI VIGILANZA .....	18

## 1. PREMESSA

La presente policy (la "Policy") illustra i principi e le misure adottate da Replica SIM S.p.A. (di seguito anche "Replica", la "Società" o la "SIM") in materia di sistemi interni di segnalazione delle violazioni, o whistleblowing, coerentemente con il quadro normativo vigente.

In via generale, attraverso il whistleblowing i dipendenti e collaboratori di una società, come di seguito meglio individuati, segnalano, a specifici individui o organismi, un reato, un illecito o qualunque condotta irregolare, commessa da altri soggetti appartenenti all'organizzazione.

La finalità del whistleblowing è quindi quella di consentire alle organizzazioni di affrontare tempestivamente il problema segnalato, contribuendo alla prevenzione e al contrasto di eventuali illeciti.

La presente Policy è adottata nel rispetto del quadro normativo applicabile alle SIM, di seguito sinteticamente illustrato.

Con riferimento all'ambito antiriciclaggio, l'articolo 2 del Decreto Legislativo 25 maggio 2017, n. 90 che modifica, dando attuazione in ambito nazionale alla Direttiva (UE) 849/2015 (c.d. "IV Direttiva Antiriciclaggio"), il Decreto Legislativo 21 novembre 2007, n. 231, introduce l'obbligo di adozione del sistema di segnalazione di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento al terrorismo. In particolare, è previsto che tale sistema garantisca la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni e la tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie o sleali conseguenti la segnalazione.

Inoltre, deve essere previsto uno specifico canale di segnalazione anonimo e indipendente, proporzionato alla natura e alle dimensioni del soggetto obbligato.

Oltre a quanto sopra delineato, a seguito dell'entrata in vigore del Decreto Legislativo 3 agosto 2017, n. 129, sono stati introdotti del Decreto Legislativo del 24 febbraio 1998, n. 58 ("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, da parte del personale, agli atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta.

In particolare, l'articolo 4-undecies del TUF prevede che gli intermediari adottino procedure specifiche per la segnalazione al proprio interno, da parte del personale, di atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta, incluse quelle in tema di abusi di mercato, e ne individua gli elementi necessari in termini di garanzie e tutele dei soggetti segnalanti.

Il medesimo articolo prevede inoltre che la Banca d'Italia e la Consob, secondo le rispettive competenze, adottino le necessarie disposizioni attuative.

Al riguardo, si evidenzia che la Banca d'Italia ha emanato, in data 5 dicembre 2019, il *"Regolamento di attuazione degli articoli 4-undecies, e 6, comma 1, lettere b) e c-bis, del TUF"* che, ai sensi del combinato disposto degli articoli 39 e 9, prevede che *"l'organo con funzione di supervisione strategica approva i sistemi interni di segnalazione delle violazioni"*.

L'articolo 4-duodecies del TUF prevede, invece, che la Banca d'Italia e la Consob ricevano, ciascuna per le materia di propria competenza, da parte del personale dei soggetti indicati dall'art. 4-undecies del TUF, le segnalazioni che si riferiscono a violazioni delle norme del TUF, nonché di atti della UE direttamente applicabili nelle stesse materie.

Ancora, il 29 dicembre 2017 è entrata in vigore la legge n. 179 *"Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"*, che mira a incentivare la collaborazione dei lavoratori per favorire l'emersione di fenomeni corruttivi all'interno di enti pubblici e privati.

Successivamente, in attuazione della Direttiva (UE) 2019/1937, concernente la protezione delle persone che segnalano violazioni del diritto dell'Unione, è stato emanato il D.lgs. n. 24 del 10 marzo 2023 (di seguito "d.lgs. 24/2023" o "Decreto Whistleblowing"), le cui disposizioni hanno avuto effetto a partire dal 15 luglio 2023.

Alla luce di quanto disposto dall'art. 2, lett. q), n. 2, del Decreto Whistleblowing, la SIM rientra nell'ambito di applicazione del suddetto Decreto in quanto soggetto sottoposto agli atti dell'Unione Europea in materia di servizi finanziari e, pertanto, essa si è dotata della presente Policy, al fine di regolare il nuovo canale di segnalazione implementato dalla stessa Società.

Coerentemente con il quadro normativo appena descritto, la presente Policy disciplina:

- a) il funzionamento di un canale interno (mediante Piattaforma) per l'effettuazione delle segnalazioni;
- b) la tutela dei soggetti segnalanti e dei soggetti coinvolti dalla segnalazione;
- c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione nonché degli altri soggetti ai quali è estesa la tutela contro gli atti ritorsivi e/o discriminatori sulla base di quanto previsto dal quadro normativo di riferimento;
- d) la previsione di sanzioni nei confronti di chi viola le misure di tutela del segnalante;
- e) la previsione di sanzioni nei confronti di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate;
- f) l'adempimento di alcuni oneri di pubblicità introdotti dal quadro legislativo;
- g) il funzionamento del canale esterno alle Autorità di Vigilanza (Banca d'Italia e Consob).

## 2. OBIETTIVI

La presente Policy mira a disciplinare il processo di segnalazione interna di Replica SIM S.p.A. (di seguito anche “**Replica**”, la “**Società**” o la “**SIM**”) in conformità a quanto previsto ai sensi dell’art. 4 del D.lgs. n. 24/2023 e dell’art. 4- *undecies* del TUF, regolando, nello specifico:

- h) il processo di ricezione, analisi e trattamento delle segnalazioni (di seguito, anche “gestione della segnalazione”) è effettuato attraverso l’attivazione di un portale dedicato - “Portale Whistleblowing” o “Portale” - idoneo a garantire, con modalità informatiche, la sicurezza dell’intero processo istruttorio e la riservatezza dell’identità dei segnalanti;
- i) il processo di ricezione, analisi e trattamento delle segnalazioni prese in carico da un soggetto diverso da quello previsto, qualora quest’ultimo si trovi in una condizione di conflitto di interessi;
- j) il processo di ricezione, analisi e trattamento delle segnalazioni mediante il canale alternativo della formulazione in forma orale della segnalazione. Quest’ultima è effettuata sempre attraverso il Portale, mediante il sistema di messaggistica vocale ivi integrato;
- k) il processo di segnalazione esterno alle Autorità di Vigilanza ai sensi di quanto previsto dall’art. art. 4-*duodecies* del TUF;

La presente policy non disciplina:

- l) la Segnalazione Esterna all’ANAC, in quanto direttamente prevista e regolata dalle disposizioni di legge di cui al citato d.lgs. 24/2023 (cfr. articoli 6 – 11). In dettaglio, la richiamata normativa: i) indica i presupposti per poter procedere alla segnalazione esterna (art. 6); ii) descrive i canali per la segnalazione esterna (art. 7); iii) identifica e regola le attività dell’ANAC, quale destinataria delle menzionate segnalazioni (art. 8); iv) prevede doveri di trasparenza dell’ANAC (art. 9); v) contempla il potere/dovere dell’ANAC di emanare in materia apposite linee guida per la presentazione e la gestione delle segnalazioni della specie.

Tuttavia, in ossequio alle disposizioni previste all’art. 5, comma 1, lett. e), del D.lgs. n. 24/2023 la presente policy prevede le condizioni per poter accedere alla Segnalazione Esterna da indirizzare all’ANAC, ovvero:

- m) non è prevista, nell’ambito del suo contesto lavorativo, l’attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dalla legge;
- n) la persona segnalante ha già effettuato una segnalazione interna ai sensi

dell'articolo 4 del D.lgs. n. 24/2023 e la stessa non ha avuto seguito;

- o) la persona segnalante 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;
- p) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- q) la Divulgazione Pubblica, direttamente regolata dal menzionato d.lgs. 24/2023, all'art. 15.

### 3. DEFINIZIONI

**ANAC:** Autorità Nazionale Anticorruzione;

**Canale di Segnalazione Interna:** canale interno di segnalazione attivato dalla SIM tramite la piattaforma dell'outsourcer DigitalPA rintracciabile al seguente indirizzo web: <https://replicasim.segnalazioni.net/>.

**CdA:** Consiglio di Amministrazione della SIM

**CS:** Collegio Sindacale della SIM; per quanto concerne le comunicazioni esse dovranno essere effettuate al Presidente del Collegio Sindacale;

**Destinatari:** potenziali soggetti segnalanti e destinatari della presente Policy come individuati nel paragrafo 4;

**AD:** Amministratore Delegato della SIM;

**Divulgazione Pubblica o Divulgare Pubblicamente:** 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;

**Portale Whistleblowing:** Piattaforma informatica gestita da "DigitalPA" e adottata da Replica per gestire il canale di segnalazione interno;

Responsabile Whistleblowing: il Direttore Generale della SIM;

**Segnalazione Esterna:** la comunicazione, scritta od orale, delle informazioni sulle Violazioni presentata tramite il canale di segnalazione esterna attivato dall'ANAC ai sensi dell'art. 7 del D.lgs. 24/2023

**Segnalazione Interna:** la comunicazione, scritta od orale, delle informazioni sulle Violazioni, presentata tramite il canale di segnalazione interna descritto nella presente Policy, nonché la richiesta di incontro in presenza quale modalità alternativa;

**Fascicolo della segnalazione:** fascicolo digitale interno al Portale Whistleblowing contenente le informazioni della segnalazione;

**Violazione:** comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato come meglio individuati nel par. 6 della presente Policy.

#### 4. SOGGETTI SEGNALANTI

I Destinatari della presente Policy identificati quali potenziali segnalanti, sono:

- a) i componenti degli organi sociali della SIM (i.e. i membri del Consiglio di Amministrazione, l'Amministratore Delegato, i membri del Collegio Sindacale);
- b) i lavoratori subordinati della SIM, siano essi dirigenti, quadri o impiegati (compresi rapporti di lavoro a tempo parziale, intermittente, a tempo determinato, di somministrazione, di apprendistato, di lavoro accessorio) ovvero persone con funzioni di amministrazione, direzione, controllo, anche qualora tali funzioni siano esercitate in via di mero fatto;
- c) i lavoratori autonomi, i terzi collaboratori e i dipendenti di terze società o enti che collaborino a qualsiasi titolo con la SIM;
- d) i fornitori e outsourcers che forniscono beni o servizi o che realizzano opere in favore della SIM;
- e) i liberi professionisti e consulenti che prestano la propria attività in favore della SIM;
- f) qualora presenti, i volontari e tirocinanti (retribuiti o non retribuiti), che prestano la propria attività presso la SIM;
- g) gli azionisti della SIM;

Per tutti i Destinatari le forme di tutela disciplinate al successivo paragrafo 10 si applicano anche durante il periodo di prova e anteriormente o successivamente alla costituzione del rapporto di lavoro o altro rapporto giuridico, come meglio specificato infra.

I Destinatari, a conoscenza di fatti suscettibili di segnalazione, nei termini di seguito esposti, sono invitati ad effettuare la segnalazione stessa con tempestività mediante le modalità più avanti descritte, astenendosi dall'intraprendere iniziative autonome di analisi e/o approfondimento.

#### 5. CANALE PER LE SEGNALAZIONI INTERNE

La presente Policy prevede il seguente canale per l'effettuazione delle Segnalazioni Interne:

- h) Portale Whistleblowing meglio descritto al successivo paragrafo 7, ed utilizzabile per effettuare la segnalazione sia in forma scritta sia in forma orale;
- i) incontro in presenza come meglio descritto al successivo paragrafo 9.

Le segnalazioni, effettuate, quindi, mediante il Portale Whistleblowing, sono ricevute dal Responsabile Whistleblowing, individuato nel Direttore Generale della SIM.

Qualora il segnalante ritenga che lo stesso Responsabile Whistleblowing sia in qualche modo coinvolto nella segnalazione, in quanto i comportamenti e le possibili violazioni oggetto della segnalazione possano riguardarlo direttamente o indirettamente, i predetti canali assicurano la possibilità per il segnalante di adire alternativamente il Collegio Sindacale. In particolare, solo con riguardo a tale specifica ipotesi (i.e. quando Responsabile Whistleblowing sia in qualche modo coinvolto nella segnalazione), il Segnalante potrà richiedere un incontro in presenza con il solo CS secondo la procedura di cui al successivo paragrafo 9.1.

Qualunque funzione/struttura diversa dal Responsabile Whistleblowing ovvero dal Collegio Sindacale che ricevesse per errore una segnalazione ha l'obbligo di trasmetterla immediatamente al Responsabile Whistleblowing ovvero al Collegio Sindacale (ove ricorra la circostanza di cui al precedente paragrafo), dandone contestuale notizia al segnalante.

I predetti canali e le modalità di gestione delle segnalazioni sono adeguatamente pubblicizzati nei luoghi di lavoro e sul sito internet della SIM in un'apposita sezione dedicata.

## **6. CARATTERISTICHE DELLE VIOLAZIONI E DELLE SEGNALAZIONI**

Le Violazioni che possono essere segnalate ai sensi della normativa vigente sono le seguenti: comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

- 1) illeciti amministrativi, contabili, civili o penali, che non rientrano nei successivi numeri 3, 4, 5, e 6;
- 2) illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al D.lgs. n. 24/23 ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato al D.lgs. n. 24/23, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- 3) atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;

- 4) atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
- 5) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei numeri 3), 4) e 5).

Le segnalazioni devono essere effettuate in buona fede e devono risultare chiare le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto delle stesse, la descrizione del fatto, le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati. È utile anche allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di soggetti che possano contribuire a circostanziare il più possibile quanto segnalato. Per quanto concerne le segnalazioni anonime ricevute attraverso i canali interni istituiti dalla SIM, esse saranno considerate alla stregua di segnalazioni ordinarie.

Non sono meritevoli di tutela le segnalazioni fondate su meri sospetti o 'voci di corridoio' o contenenti informazioni che il segnalante sa essere false.

## 7. PORTALE WHISTLEBLOWING

Il Portale Whistleblowing è raggiungibile tramite internet al seguente indirizzo <https://replicasim.segnalazioni.net/>.

Il Portale Whistleblowing implementato dalla SIM ha le seguenti caratteristiche principali:

- a) è dotato di avanzati sistemi di cifratura che garantiscono la protezione delle informazioni sensibili e l'identità dei segnalanti, impedendo l'accesso non autorizzato alle segnalazioni e garantendo la loro riservatezza;
- b) garantisce l'anonimato e la riservatezza, assicurando che l'identità del segnalante e le segnalazioni stesse siano strettamente separate, senza alcun collegamento evidente tra l'utente e le segnalazioni che effettua, assicurando così l'anonimato del segnalante;
- c) è sottoposto a rilasci mensili di aggiornamenti, con possibilità di maggiore frequenza se necessario, al fine di introdurre nuove funzionalità e miglioramenti tecnologici (prima del rilascio tali aggiornamenti vengono ampiamente testati su piattaforme di test specializzati);
- d) grazie al sistema di autenticazione a due fattori migliora la sicurezza e previene il furto di identità;
- e) è dotato di un sistema c.d. "multicanale": permette l'assegnazione automatica

delle segnalazioni ai Responsabili in base alla tipologia;

- f) è dotato di un fascicolo digitale – c.d. “Fascicolo della segnalazione” - che contiene tutte le informazioni relative alla segnalazione di riferimento;
- g) ha ottenuto le certificazioni ISO/IEC 27001, ISO 22301 e ISO 9001.

## **8. MODALITÀ DI TRASMISSIONE DELLE SEGNALAZIONI**

Accedendo al Portale Whistleblowing il segnalante è guidato nella compilazione di un questionario formato da domande aperte e chiuse che gli permettono di fornire gli elementi caratterizzanti la segnalazione (fatti, contesto temporale, persone coinvolte), eventualmente anche allegando files a supporto.

Tramite il Portale Whistleblowing è altresì possibile inviare una segnalazione in forma orale. Invero, il sistema permette di inviare la segnalazione allegando un messaggio vocale che sarà trasmesso con modalità distorta al fine di mantenere l'anonimato del segnalante.

Il segnalante può decidere di inviare la segnalazione in forma riservata o anonima.

Mediante la modalità di segnalazione in “*forma riservata*”, gli utenti identificabili devono registrarsi in anticipo e dopo avere creato un account, possono inviare la segnalazione. L'identità del segnalante registrato è separata dalla segnalazione, quindi questa viene inviata in forma anonima al Responsabile. Solo il Responsabile ha la capacità di collegare la segnalazione all'utente che l'ha creata e visualizzare l'identità del segnalante.

Mediante la modalità di segnalazione in “*forma anonima*”, invece, il sistema non permette di associare la segnalazione al nome del segnalante, non essendo quest'ultimo registrato.

L'accesso alle segnalazioni è gestito in modo diverso a seconda che la segnalazione sia stata inviata da un'utente registrato (forma riservata) o da un utente non registrato (anonima). Gli utenti registrati accedono tramite username e password scelti durante la registrazione, mentre gli utenti non registrati accedono utilizzando i codici generati dal sistema durante l'invio della segnalazione.

## **9. CANALI DI SEGNALAZIONE INTERNI ALTERNATIVI AL PORTALE WHISTLEBLWING**

Il canale descritto nel paragrafo precedente è relativo a segnalazioni effettuate in forma scritta oppure orale. Oltre a quanto già previsto, la Società ha attivato un ulteriore canale alternativo che assicura la possibilità di effettuare la segnalazione in forma orale ed in presenza.

## 9.1. Canale in presenza

Il segnalante può richiedere un incontro con il Responsabile Whistleblowing ovvero con il CS, che dovrà essere fissato da uno di questi ultimi entro un termine ragionevole, e comunque entro il termine massimo di 7 giorni.

L'incontro potrà essere richiesto a mezzo e-mail ai seguenti indirizzi:

- a) Incontro con il Responsabile Whistleblowing: [Responsabile\\_whistleblowing@replicasim.com](mailto:Responsabile_whistleblowing@replicasim.com);
- b) Incontro con il CS: [Presidente\\_CS@replicasim.com](mailto:Presidente_CS@replicasim.com).

I contenuti dell'incontro sono verbalizzati dal Responsabile Whistleblowing ovvero dal CS, previo consenso del segnalante. Qualora il segnalante abbia acconsentito alla verbalizzazione, può procedere a verificare, rettificare e confermare il verbale con la propria sottoscrizione. **Secondo quanto disciplinato nel precedente paragrafo 5, nell'ipotesi in cui segnalante ritenga che lo stesso Responsabile Whistleblowing sia in qualche modo coinvolto nella segnalazione, in quanto i comportamenti e le possibili violazioni oggetto della segnalazione possano riguardarlo direttamente o indirettamente, il medesimo segnalante potrà richiedere un incontro in presenza del solo CS.**

## **10. GESTIONE DELLE SEGNALAZIONI MEDIANTE PORTALE WHSITLEBLOWING**

Le segnalazioni trasmesse mediante il Portale Whistleblowing sono ricevute dal Responsabile Whistleblowing.

Per ogni segnalazione, all'interno del Portale Whistleblowing, viene creato un Fascicolo della segnalazione (c.d. Fascicolo digitale) che include le informazioni inizialmente fornite dal segnalante e successivamente arricchite tramite la c.d. l'Area Messaggi.

L'Area Messaggi è una speciale bacheca nella quale confluiscono i messaggi scambiati tra il Segnalante e il Gruppo di lavoro (Responsabile, collaboratori).

L'eventuale condivisione della segnalazione e della documentazione prodotta dal segnalante con altre funzioni aziendali o con professionisti esterni a scopo di indagine viene svolta con la massima cautela, previo oscuramento dei dati e delle informazioni che potrebbero rivelare, anche indirettamente, l'identità del segnalante e previa verifica - se applicabile - che tali soggetti siano autorizzati al trattamento dei dati personali.

Le segnalazioni sono soggette al seguente iter istruttorio.

### Analisi preliminare

Il Responsabile Whistleblowing svolge un'analisi preliminare avente il solo scopo di verificare la possibile fondatezza della segnalazione e individuare l'organo e/o il soggetto e/o la/e funzione/i interessata/e alla segnalazione medesima. Qualora la segnalazione risulti manifestamente e inequivocabilmente infondata, ne viene disposta dal Responsabile

Whistleblowing l'immediata archiviazione con annotazione della relativa motivazione e non si dà corso all'istruttoria.

Invece, le segnalazioni che risultano sufficientemente circostanziate, oltre che rilevanti ai sensi del vigente quadro normativo, sono sottoposte ad istruttoria, nel rispetto della riservatezza sull'identità del segnalante.

## Istruttoria

In fase di istruttoria, il Responsabile Whistleblowing provvede a:

- avviare approfondimenti specifici avvalendosi, se ritenuto opportuno, delle strutture competenti dell'Intermediario o di esperti esterni. In tale ambito, può essere sentita la persona coinvolta dalla segnalazione, su iniziativa del Responsabile Whistleblowing. Quest'ultimo è tenuto a sentire la persona coinvolta, qualora l'iniziativa sia assunta della stessa persona coinvolta. L'ascolto della persona coinvolta può avvenire anche sulla base di documentazione scritta (osservazioni/altra documentazione) direttamente tramite il Portale Whistleblowing;
- concordare con il management responsabile della funzione interessata dalla segnalazione, d'intesa con l'AD salvo che sia lui stesso coinvolto nella segnalazione, l'eventuale "action plan" necessario per la rimozione delle debolezze di controllo rilevate;
- proporre all'AD e alle altre funzioni interessate, con esclusione di coloro che siano coinvolti nella segnalazione, eventuali iniziative da intraprendere a tutela degli interessi di Replica (es. denuncia all'Autorità Giudiziaria, procedimenti disciplinari a carico della persona coinvolta, sospensioni/cancellazioni di fornitori dall'Albo fornitori, risoluzioni contrattuali, ecc.);
- proporre all'AD e al Manager Responsabile della Funzione interessata salvo che siano coinvolti nella segnalazione<sup>1</sup>, se necessario, l'avvio di un procedimento disciplinare nei confronti del segnalante, nel caso di segnalazioni in relazione alle quali siano accertate la malafede del segnalante e/o l'intento meramente diffamatorio, eventualmente confermati anche dalla infondatezza della segnalazione;
- alla conclusione dell'approfondimento svolto, sottoporre i risultati alla valutazione dell'AD, del Manager Responsabile della Funzione interessata o del CS, a seconda dell'oggetto della segnalazione e con esclusione di coloro che siano coinvolti nella segnalazione, affinché vengano intrapresi i più opportuni provvedimenti;
- concludere l'istruttoria in qualunque momento se, nel corso dell'istruttoria

---

<sup>1</sup> Nel caso in cui il Responsabile Whistleblowing risulti coinvolto, valgono le indicazioni di cui ai paragrafi 5 e 9.1.

medesima, sia accertata l'infondatezza della segnalazione, fatto salvo quanto previsto dal successivo punto;

- concordare con il CS eventuali iniziative da intraprendere a tutela di Replica, prima della chiusura della segnalazione stessa.

Le attività sopra descritte non sono necessariamente svolte in maniera sequenziale.

In ogni caso, entro 3 mesi dalla data di avviso di ricevimento (o, in mancanza di tale avviso, entro 3 mesi dalla scadenza del termine dei 7 giorni dalla presentazione della segnalazione), il Responsabile Whistleblowing deve fornire al segnalante un riscontro sul processo di segnalazione, ad esempio comunicando l'archiviazione della stessa, l'avvio di un'inchiesta interna ed eventualmente delle relative risultanze, dei provvedimenti adottati per affrontare la questione sollevata, nel rinvio a un'autorità competente per ulteriori indagini. Il predetto riscontro, da inviare nel termine di 3 mesi, può anche essere meramente interlocutorio, laddove il processo risulti ancora in corso; in questo caso saranno comunicate le informazioni relative a tutte le attività sopra descritte che si intende intraprendere e lo stato di avanzamento dell'istruttoria. In ogni caso, terminata l'attività istruttoria gli esiti della stessa dovranno comunque essere comunicati al segnalante.

### Registrazione

Il Responsabile Whistleblowing provvede a tenere un Registro delle Segnalazioni ove vengono annotate tutte le segnalazioni ricevute.

Le segnalazioni pervenute tramite il Portale di riferimento vengono registrate automaticamente dal sistema.

## **11. TUTELA E RESPONSABILITÀ DEL SEGNALANTE**

Al segnalante sono riconosciute misure di protezione, al ricorrere delle seguenti condizioni:

- a) al momento della segnalazione, la persona segnalante aveva fondato motivo di ritenere che le informazioni sulle Violazioni segnalate fossero vere e rientrassero nell'ambito oggettivo previsto dal D.lgs. 24/2023;
- b) la segnalazione è stata effettuata sulla base di quanto previsto dal D.lgs. 24/2023.

I motivi che hanno indotto la persona a segnalare o denunciare o divulgare pubblicamente sono irrilevanti ai fini della sua protezione.

Pertanto, è assicurata la tutela:

- c) della riservatezza della propria identità, riferita non solo al nominativo, ma anche a tutti gli elementi della segnalazione, inclusa la documentazione ad essa allegata, il cui disvelamento, anche indirettamente, possa consentire l'identificazione del segnalante.

Nel dettaglio:

- l'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;
  - nell'ambito del procedimento penale, l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale;
  - nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa del segnalato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità;
  - Qualora il ricevente debba comunicare l'identità del segnalante perché rilevante per la difesa della persona coinvolta/incolpata, nei casi sopra considerati, deve comunicare al segnalante delle motivazioni e raccogliere il suo consenso scritto prima di procedere alla comunicazione dell'identità del segnalante;
- d) contro misure ritorsive o discriminatorie, dirette o indirette, adottate a seguito della segnalazione effettuata in buona fede, quali, a titolo non esaustivo, sanzioni disciplinari, demansionamento, licenziamento, trasferimento, peggioramento delle condizioni di lavoro. Per misure ritorsive si intende qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto;
- e) attraverso misure di sostegno previste dal D.lgs. n. 24/23.

Il segnalante potrà altresì denunciare eventuali comportamenti ritorsivi, che ritiene di avere subito, all'ANAC come previsto dal D.lgs. 24/2023 (c.d. Segnalazione Esterna).

La protezione, ivi compresa la tutela contro misure ritorsive, è assicurata da Replica anche al segnalante anonimo allorché, nell'ambito della gestione della segnalazione, emerge successivamente l'identità del segnalante.

Quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele di cui al presente capo non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare.

Il sistema disciplinare di Replica prevede sanzioni:

- nei confronti di chi viola le misure di tutela del segnalante. Sanzioni pecuniarie contro i comportamenti ritorsivi sono altresì previste dal D.lgs. n. 24/23 e applicate dall'ANAC;
- nei confronti del segnalante che effettui con dolo o colpa grave segnalazioni che si rivelino false, infondate, con contenuto diffamatorio o comunque effettuate al solo scopo di danneggiare l'Intermediario, il segnalato o altri soggetti interessati dalla segnalazione.

La SIM potrà inoltre intraprendere le opportune iniziative anche in sede giudiziale.

La tutela del segnalante concerne il segnalante anche:

- qualora il rapporto giuridico lavorativo non sia 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.

## **12. ESTENSIONE DELLA TUTELA DEL SEGNALANTE AD ALTRI SOGGETTI**

Le misure di protezione, sopra richiamate per il segnalante, si applicano altresì:

- a) ai c.d. facilitatori delle segnalazioni. Per facilitatore della segnalazione, la Legge intende una *“persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata”*;
- b) alle persone del medesimo contesto lavorativo della persona segnalante e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- c) 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;
- d) agli enti di proprietà – in via esclusiva o in compartecipazione maggioritaria di terzi - della persona segnalante o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

## **13. TUTELA DEL SEGNALATO**

Al segnalato è riconosciuta la tutela della riservatezza della propria identità, al fine di evitare conseguenze pregiudiziali, anche solo di carattere reputazionale, all'interno del

contesto lavorativo in cui opera. La segnalazione non è sufficiente ad avviare alcun procedimento disciplinare verso il segnalato.

Qualora, a seguito di concreti riscontri acquisiti a riguardo della segnalazione, si decida di procedere con l'attività istruttoria, il segnalato potrà essere contattato dal Responsabile Whistleblowing e gli verrà assicurata la possibilità di fornire ogni eventuale e necessario chiarimento.

La tutela del segnalato si applica fatte salve le previsioni di legge che impongono l'obbligo di comunicare il nominativo del soggetto segnalato sospettato di essere responsabile della violazione (ad esempio richieste dell'Autorità giudiziaria).

#### **14. REPORTISTICA**

Con cadenza annuale, il Responsabile Whistleblowing elabora una relazione riepilogativa delle segnalazioni pervenute da sottoporre all'attenzione del CdA e del CS.

#### **15. CONSERVAZIONE DELLA DOCUMENTAZIONE**

Il Responsabile Whistleblowing o il CS curano l'archiviazione di tutta la documentazione relativa al whistleblowing e tengono periodicamente aggiornato il Registro delle Segnalazioni.

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del D.lgs. n. 24/23 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del Decreto legislativo n. 51 del 2018.

#### **16. PROTEZIONE DEI DATI PERSONALI**

Ogni trattamento dei dati personali deve essere effettuato a norma del regolamento (UE) 2016/679, del Decreto legislativo 30 giugno 2003, n. 196 e Del decreto legislativo 18 maggio 2018, n. 51.

##### **a) Rispetto del principio di necessità**

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente. I diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

##### **b) Riconoscimento dei diritti privacy**

I trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni sono effettuati dalla SIM, in qualità di titolare del trattamento, nel rispetto dei principi di cui agli

articoli 5 e 25 del regolamento (UE) 2016/679 o agli articoli 3 e 16 del Decreto legislativo n. 51 del 2018, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato Decreto legislativo n. 51 del 2018, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

Al soggetto segnalato sono riconosciuti i diritti di cui agli artt. 15 e ss. del Reg. (UE) 2016/679<sup>2</sup> nei limiti di cui all'art. 2-undecies del D.lgs. 196/2003 ovvero - in particolare - ad eccezione dei casi in cui dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto: “[...] *ff) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio*”. Il soggetto segnalato ha in ogni caso facoltà di esercitare tali diritti anche tramite il Garante per la Protezione dei Dati Personali, con le modalità di cui all'art. 160 del D.lgs. 196/2003.

### **c) Non applicabilità dell'accesso agli atti**

Le segnalazioni sono sottratte all'accesso previsto dagli articoli 22 e segg. della legge 7 agosto 1990, n. 241, nonché dagli articoli 5 e seguenti del Decreto legislativo 14 marzo 2013, n. 33.

## **17. ONERI DI PUBBLICITÀ PER REPLICA SIM A FINI DI TRASPARENZA DEL WHISTLEBLOWING**

La SIM assicura adeguata pubblicità alle modalità di effettuazione delle segnalazioni interne, previste dalla presente Policy, e delle segnalazioni esterne e divulgazioni pubbliche previste dal D.lgs. 24/2023.

La SIM, pertanto:

- a) assicura adeguata diffusione interna alla presente Policy, al pari di tutta l'altra normativa interna;
- b) prevede la consegna della presente Policy, unitamente ai principali documenti di normativa interna, ai propri collaboratori, consulenti e fornitori di servizi (outsourcer), stagisti, remunerati e non remunerati;
- c) pubblica sul proprio sito internet, nell'apposita sezione dedicata, le modalità attraverso cui effettuare le segnalazioni interne e le condizioni previste dal D.lgs. n. 24/2023 per le segnalazioni esterne e le divulgazioni pubbliche.

---

<sup>2</sup> Si tratta nello specifico del diritto di accesso ai dati personali (art. 15 GDPR), del diritto a rettificarli (art. 16 GDPR), del diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio (art. 17 GDPR), del diritto alla limitazione del trattamento quando ricorrono le ipotesi specificate dall'art. 18 GDPR, del diritto alla portabilità dei dati personali (art. 20 GDPR) e di quello di opposizione al trattamento (art. 21 e 22 GDPR).

<sup>3</sup> Tale norma prevede la possibilità per l'interessato di richiedere al Garante accertamenti sulla conformità del trattamento dei propri dati.

## 18. IL CANALE DI SEGNALAZIONE ESTERNA ALL'AUTORITÀ DI VIGILANZA

Ai sensi di quanto previsto dall'art. 1 del D.lgs. 24/2023, le disposizioni ivi contenute non si applicano tra l'altro, *“alle segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione Europea o nazionale indicati nella parte II dell'allegato al decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II”* del Decreto Whistleblowing.

Pertanto, nel caso di violazioni delle norme disciplinanti l'attività svolta dalla SIM, incluse quelle in tema di abusi di mercato, oltre al canale di Segnalazione Interno già delineato, il segnalante può effettuare le segnalazioni tramite il canale esterno predisposto dall'Autorità di Vigilanza in conformità alle regole operative da loro definite (cfr. art. 4-duodecies del TUF), per effettuare le segnalazioni opportune.

In particolare, con riferimento alla Consob, sul sito internet dell'Autorità<sup>4</sup> sono indicate le modalità operative per trasmettere direttamente alla Consob segnalazioni riferite a presunte violazioni o illeciti delle norme del TUF nonché degli atti dell'Unione europea direttamente applicabili nelle stesse materie. Sono garantite tutte le tutele degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro, in conformità con le previsioni di cui alla Legge 30 novembre 2017, n. 179, tra cui l'illegittimità di eventuali provvedimenti di tipo disciplinare con finalità ritorsive o discriminatorie del soggetto segnalante.

Le segnalazioni alla Banca d'Italia sono invece trasmesse attraverso l'apposito modulo presente nel sito internet<sup>5</sup> e possono essere inviate tramite la piattaforma "Servizi online", selezionando il box "Invia una segnalazione" sul sito internet dell'Autorità, ovvero via posta ordinaria, all'indirizzo della Banca d'Italia – Servizio RIV – divisione SRE – a Roma, Via Nazionale n. 91, con busta recante la dicitura “riservato”.

La Banca d'Italia si riserva – ove lo ritenga opportuno – di contattare il segnalante per ottenere ulteriori informazioni o chiarimenti, in osservanza al segreto d'ufficio che copre tutti i dati e le informazioni o notizie acquisiti in ragione dell'attività di vigilanza.

La Banca d'Italia assicura la riservatezza dei dati personali del segnalante, anche al fine di assicurare quest'ultimo da possibili ritorsioni.

---

<sup>4</sup> <https://www.consob.it/web/area-pubblica/whistleblowing>

<sup>5</sup> <https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/index.html>