Sistema di Gestione del Whistleblowing

REV. 01 – 20.10.2026

Rev.	Data	Descrizione	Approvazione
00	8.11.2024	Prima emissione	AU – 8.11.2024
01	20.10.2026	Seconda emissione – adozione canale crittografato	

INDICE

1. IL WHISTLEBLOWING 3
2. I SOGGETTI TUTELATI - I WHISTLEBLOWERS 3
2.1. I soggetti segnalanti 3
2.2. Altri soggetti meritevoli di protezione 4
3. OGGETTO DELLE SEGNALAZIONI 4
3.1. Segnalazioni escluse o non ammissibili 5
4. LE SEGNALAZIONI RILEVANTI 5
5. LA PROCEDURA DI SEGNALAZIONE INTERNA 6
5.1. Modalità della segnalazione 6
5.2. Segnalazioni anonime 6
5.3. Segnalazioni ricevute da soggetti diversi dal Gestore 6
5.4. Il Gestore della segnalazione interna. Esecuzione dell'istruttoria 7
5.5. Conflitto di interessi e continuità 7
5.6. Istruttoria e decisione 8
6. LA PROCEDURA DI SEGNALAZIONE ESTERNA TRAMITE ANAC 9
6.1. Condizioni per la segnalazione esterna 9
7. LA SEGNALAZIONE TRAMITE DIVULGAZIONE PUBBLICA E DENUNCIA 9
8. IL REGIME DI PROTEZIONE PER I SEGNALANTI 10
8.1. Il divieto di ritorsioni e l'onere della prova 10
8.2. Protezione dalle ritorsioni e ruolo di ANAC 11
8.3. Riservatezza e relativi limiti 11
8.4. Tutela della persona coinvolta 12
9. LA CONSERVAZIONE DELLA DOCUMENTAZIONE 12
10. IL TRATTAMENTO DEI DATI 13
11. IL SISTEMA SANZIONATORIO 14
11.1. Le sanzioni previste da ANAC 14
11.2. Sanzioni prevista da Sider Sipe S.p.A. 14
12. COORDINAMENTO CON MODELLO 231, ODV E FLUSSI INFORMATIVI 15
13. FORMAZIONE, INFORMAZIONE, REPORTING E MONITORAGGIO 15

1. IL WHISTLEBLOWING

Il whistleblowing è uno strumento di compliance aziendale, che consente ai soggetti che operano o hanno operato nel contesto lavorativo della Società di segnalare in modo protetto e riservato, eventuali illeciti o irregolarità riscontrati durante la propria attività lavorativa.
La disciplina si collega al tema della gestione delle informazioni all'interno degli enti e trova collocazione nell'ambito degli strumenti di controllo interno in funzione di prevenzione degli illeciti.
Il whistleblowing rappresenta, inoltre, una forma di collaborazione doverosa per il dipendente, volta a rafforzare la cultura della trasparenza e dell'integrità degli enti pubblici e privati in funzione di tutela dell'interesse pubblico.
In Italia, il whistleblowing è regolato dal decreto legislativo 10 marzo 2023, n. 24 che ha disposto in un unico testo normativo, per il settore pubblico e privato, la disciplina della protezione dei soggetti che segnalano (non in forma anonima) violazioni di disposizioni europee e nazionali di cui sono venuti a conoscenza nel contesto lavorativo e che ledono gli interessi pubblici o dell'integrità degli enti di appartenenza.

2. I SOGGETTI TUTELATI - I WHISTLEBLOWERS

La disciplina del whistleblowing prevede due categorie di soggetti cui si applicano le tutele:

- Il "**segnalante**", cioè la persona fisica che effettua la segnalazione e la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo;
- **gli altri soggetti** che, pur non avendo effettuato direttamente la segnalazione, sono comunque ritenuti meritevoli di protezione

La tutela opera quando, al momento della segnalazione, denuncia o divulgazione pubblica, il segnalante aveva fondato motivo di ritenere che le informazioni fossero vere e rientrassero nell'ambito oggettivo della disciplina. Non operano le tutele in caso di segnalazioni dolosamente false o gravemente colpose, ferma la necessità dell'accertamento nelle sedi competenti.

2.1. I soggetti segnalanti

Tra i soggetti legittimati a effettuare segnalazioni rientrano coloro che hanno acquisito informazioni sulle violazioni nell'ambito del proprio contesto lavorativo, anche quando il rapporto giuridico non sia ancora iniziato, sia in corso o sia cessato, purché le informazioni siano state acquisite in occasione del rapporto stesso o nella fase precontrattuale, nel dettaglio:

- lavoratori subordinati, anche a tempo determinato o parziale, e lavoratori e collaboratori di fornitori di beni o servizi e di soggetti che realizzano opere in favore della Società;
- lavoratori autonomi, collaboratori, consulenti e liberi professionisti che prestano attività in favore della Società;
- volontari e tirocinanti, anche non retribuiti;
- azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche esercitate di fatto;
- candidati, persone in fase di selezione o trattativa precontrattuale, lavoratori in prova ed ex lavoratori o collaboratori, nei limiti delle informazioni acquisite nel contesto lavorativo previsto dalla legge.

2.2. Altri soggetti meritevoli di protezione

Le tutele sono estese anche ai soggetti che, pur non essendo autori della segnalazione, possono subire ritorsioni in ragione del collegamento con il segnalante. In particolare:

- facilitatori: persone fisiche che assistono il segnalante nel processo di segnalazione, operano nel medesimo contesto lavorativo e la cui assistenza deve restare riservata;
- persone del medesimo contesto lavorativo legate al segnalante da stabile legame affettivo o di parentela entro il quarto grado;
- colleghi che lavorano nel medesimo contesto lavorativo del segnalante e hanno con lui un rapporto abituale e corrente;
- enti di proprietà del segnalante, della persona che denuncia o divulga pubblicamente, enti per i quali tali persone lavorano ed enti operanti nel medesimo contesto lavorativo, alle condizioni dell'art. 3, comma 5, del decreto. I collegamenti di cui ai punti precedenti rilevano anche rispetto a chi denuncia o divulga pubblicamente.

La tutela opera anche in caso di segnalazioni anonime qualora il segnalante sia successivamente identificato e subisca ritorsioni, purché la segnalazione sia stata effettuata nel rispetto delle condizioni previste dalla normativa e dal presente Sistema.

3. OGGETTO DELLE SEGNALAZIONI

Sono oggetto di segnalazione i comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità della Società e di cui il segnalante sia venuto a conoscenza nel contesto lavorativo.
La segnalazione può riguardare violazioni già commesse, condotte in corso, fondati sospetti relativi a violazioni che potrebbero essere commesse sulla base di elementi concreti, nonché condotte dirette a occultare la violazione o a impedire l'accertamento dei fatti.
A titolo esemplificativo, sono segnalabili:

- presunti reati presupposto previsti dal del D. Lgs. 231/2001 e violazioni del Modello di Organizzazione, Gestione e Controllo, del Codice Etico o dei protocolli aziendali;
- illeciti commessi in violazione della normativa dell'Unione europea e delle disposizioni nazionali di attuazione nei settori indicati dal D. Lgs. 24/2023, tra cui contratti pubblici, servizi finanziari, prevenzione del riciclaggio e del finanziamento del terrorismo, sicurezza dei prodotti, sicurezza dei trasporti, tutela dell'ambiente, salute pubblica, protezione dei consumatori, protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- atti od omissioni lesivi degli interessi finanziari dell'Unione europea;
- atti od omissioni riguardanti il mercato interno, comprese violazioni in materia di concorrenza, aiuti di Stato e imposta sulle imprese;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione nei settori sopra indicati;
- violazioni delle misure restrittive dell'Unione europea.

3.1. Segnalazioni escluse o non ammissibili

Sono escluse le contestazioni, rivendicazioni o richieste legate a un interesse personale che attengono esclusivamente al rapporto individuale di lavoro o ai rapporti con superiori. La presenza di un interesse personale non esclude una segnalazione che riguardi anche una violazione compresa nel decreto.
Sono altresì escluse le segnalazioni manifestamente infondate, generiche, prive di elementi di fatto idonei a consentire verifiche, basate su mere voci o indiscrezioni, nonché le segnalazioni effettuate con dolo o colpa grave allo scopo di danneggiare la persona coinvolta o la Società.

Restano ferme le discipline speciali, ove applicabili, in materia di informazioni classificate, segreto professionale, segreto medico e forense, segretezza delle deliberazioni degli organi giurisdizionali, norme di procedura penale e tutela della difesa nazionale e dell'ordine e sicurezza pubblica.

4. LE SEGNALAZIONI RILEVANTI

Le segnalazioni prese in considerazione sono quelle circostanziate, fondate su elementi precisi e concordanti e riferite a fatti direttamente conosciuti dal segnalante nel contesto lavorativo.

Il canale whistleblowing non deve essere utilizzato per finalità meramente personali, rivendicative o ritorsive.

Perché la segnalazione sia meritevole di considerazione è necessario che:

- la violazione rientri nell'ambito oggettivo di applicazione della normativa e possa pregiudicare l'interesse pubblico o l'integrità della Società;
- sussistano fondati motivi per ritenere che l'informazione sia vera;
- la segnalazione sia circostanziata e fondata su elementi precisi e, ove possibile, documentabili;
- la violazione sia riscontrabile attraverso verifiche proporzionate e legittime;
- la segnalazione contenga informazioni utili a individuare gli autori della condotta, le funzioni coinvolte e le circostanze rilevanti.

Il segnalante deve indicare, ove possibile, le seguenti informazioni:

a) data, luogo, modalità e circostanze dei fatti;
b) generalità o elementi identificativi dei soggetti coinvolti;
c) documenti, comunicazioni, dati o altri riscontri disponibili;
d) nominativi di persone informate;
e) modalità con cui è venuto a conoscenza dei fatti;
f) eventuali interessi privati collegati alla segnalazione.

5. LA PROCEDURA DI SEGNALAZIONE INTERNA

I canali di segnalazione interna sono strutturati in modo da assicurare la riservatezza dell'identità del segnalante, del facilitatore, delle persone coinvolte, del contenuto della segnalazione e della documentazione allegata.
Il Sistema si ispira ai principi di riservatezza, segregazione e *need to know*, tracciabilità, imparzialità e indipendenza del Gestore, protezione da ritorsioni, *data protection by design e by default*, buona fede e responsabilità.
La Società assicura la disponibilità di modalità scritta e orale.
La scelta della modalità spetta al segnalante.
Laddove il canale sia istituito o modificato in modo sostanziale, ovvero siano coinvolti provider o gestori esterni, l'assetto deve essere formalizzato mediante atto organizzativo o aggiornamento del Modello 231, previa informativa alle rappresentanze sindacali ove presenti e secondo quanto previsto dalla normativa applicabile.

5.1. Modalità della segnalazione

Canale	Modalità	Presidio di riservatezza	Indicazioni operative
Piattaforma informatica	Scritta e, ove disponibile, messaggio vocale	Crittografia, segregazione dati, accesso riservato al Gestore, tracciabilità ed eventuale anonimizzazione	**Link:** https://sidersipe.segnalazioni.net/ Il segnalante deve conservare il codice univoco rilasciato dalla piattaforma per seguire lo stato della pratica e rispondere a richieste di integrazione.
Canale orale dedicato	Linea telefonica o sistema di messaggistica vocale, se attivato	Registrazione o trascrizione solo previo consenso; conservazione su supporto idoneo; eventuale alterazione voce e rimozione metadati se gestito tramite piattaforma	A prescindere dal canale orale dedicato, il segnalante può richiedere un incontro diretto tramite piattaforma o altro canale riservato.
Incontro diretto	Orale in presenza o da remoto con modalità protetta	Verbale o registrazione previo consenso; possibilità per il segnalante di verificare, rettificare e confermare il verbale	L'incontro è fissato entro un termine ragionevole dalla richiesta e gestito in luogo o modalità idonei a preservare la riservatezza.

5.2. Segnalazioni anonime

La Società ammette segnalazioni anonime quando risultino adeguatamente circostanziate e fondate su elementi di fatto sufficientemente dettagliati da consentire verifiche.
Le segnalazioni anonime sono registrate e conservate dal Gestore con modalità tali da garantire tracciabilità, riservatezza e tutela in caso di successiva identificazione del segnalante.
La Società incoraggia comunque, ove possibile, l'utilizzo della segnalazione nominativa, in ragione della maggiore efficacia dell'interlocuzione con il segnalante e della possibilità di acquisire chiarimenti e integrazioni.

5.3. Segnalazioni ricevute da soggetti diversi dal Gestore

Chiunque, diverso dal Gestore, riceva una segnalazione, in qualunque forma, deve trasmetterla tempestivamente e comunque entro 3 giorni dal ricevimento al Gestore, utilizzando modalità riservate e dando contestuale notizia della trasmissione al segnalante, ove noto. È vietato

trattenere copie, avviare autonome verifiche o diffondere informazioni relative alla segnalazione.

La violazione dell'obbligo di trasmissione e riservatezza costituisce illecito disciplinare e può comportare l'applicazione delle sanzioni previste dal presente Sistema e dal Modello 231.

5.4. Il Gestore della segnalazione interna. Esecuzione dell'istruttoria

Il Gestore della Segnalazione interna è il soggetto incaricato di ricevere, prendere in carico, valutare, istruire e definire le segnalazioni interne.
Il Gestore deve possedere autonomia, imparzialità e competenze adeguate in materia di whistleblowing, Modello 231, gestione istruttoria, riservatezza e protezione dei dati personali.
Il Gestore può avvalersi, ove necessario, del supporto di funzioni aziendali o consulenti esterni, nel rispetto del principio del *need to know*, previa adozione di misure idonee a preservare la riservatezza del segnalante e delle persone coinvolte. Il coinvolgimento di soggetti terzi deve essere documentato nel fascicolo della segnalazione.
Sider Sipe S.p.A. ha conferito l'incarico di Gestore delle Segnalazioni Whistleblowing all'Avv. Andrea Peluso.

5.5. Conflitto di interessi e continuità

Qualora la segnalazione riguardi il Gestore, un suo componente, un soggetto strettamente collegato al Gestore oppure fatti rispetto ai quali il Gestore versi in una situazione di conflitto anche solo potenziale, la gestione deve essere assegnata a un soggetto supplente autonomo e competente individuato dall'organo amministrativo o secondo il presidio preventivamente deliberato.

Soggetto supplente in caso di conflitto: **Sig.ra Anna Guzzetta**

Le segnalazioni che coinvolgono il Gestore sono indirizzate direttamente al sostituto all'indirizzo **annaguzzetta@postecert**, senza accesso del Gestore al fascicolo.

Il Gestore, in particolare, è tenuto a:

- rilasciare al segnalante l'avviso di ricevimento entro 7 giorni dalla ricezione della segnalazione;
- mantenere interlocuzioni con il segnalante, richiedendo integrazioni ove necessario;
- dare diligente seguito alla segnalazione, verificando ammissibilità, fondatezza e misure conseguenti;
- fornire riscontro entro 3 mesi dall'avviso di ricevimento;
- documentare le attività svolte e garantire la tracciabilità del processo;
- proteggere identità, contenuto della segnalazione, documentazione allegata e dati personali;
- monitorare l'assenza di ritorsioni, ove possibile e pertinente;

- informare gli organi competenti quando siano necessarie misure correttive, disciplinari, organizzative o di segnalazione all'autorità.

5.6. Istruttoria e decisione

Fase	Attività	Termine/Output	Responsabile
Ricezione	Acquisizione della segnalazione attraverso piattaforma, posta riservata, canale orale o incontro diretto; registrazione nel fascicolo riservato.	Avviso di ricevimento entro 7 giorni.	Gestore
Valutazione preliminare	Verifica di ammissibilità, competenza, pertinenza whistleblowing, sufficiente descrizione delle circostanze, eventuale conflitto di interessi.	Archiviazione motivata o apertura istruttoria.	Gestore
Interlocuzione	Richiesta di chiarimenti, integrazioni o documenti al segnalante, se possibile.	Tracciamento comunicazioni in piattaforma/fascicolo.	Gestore
Istruttoria	Piano di indagine, acquisizione documenti, audizioni, analisi dati, coinvolgimento funzioni o consulenti, separazione dati identificativi.	Relazione istruttoria riservata.	Gestore con eventuale supporto
Decisione	Valutazione esiti, proposta di archiviazione, azioni correttive, misure disciplinari, trasmissione a organi o autorità competenti.	Entro 3 mesi dall'avviso o, se manca, dalla scadenza dei 7 giorni dalla presentazione.	Gestore per esito; organi competenti non coinvolti per misure.
Follow-up	Verifica attuazione misure, aggiornamento fascicolo, monitoraggio assenza ritorsioni.	Chiusura motivata e conservazione.	Gestore

Il Gestore verifica preliminarmente se la segnalazione rientra nel perimetro del D.Lgs. 24/2023 e della presente procedura, se contiene elementi sufficienti per procedere, se richiede integrazioni e se sussistono profili di urgenza o rischio di ritorsioni, occultamento prove o reiterazione della condotta.

In caso di segnalazione manifestamente infondata, generica, inammissibile o estranea al perimetro whistleblowing, il Gestore dispone l'archiviazione motivata, ferma la possibilità di indirizzare il segnalante verso canali aziendali ordinari, ove esistenti e senza pregiudizio per la riservatezza.

Quando la segnalazione è ammissibile, il Gestore definisce un piano di istruttoria proporzionato alla natura e complessità dei fatti. Le attività istruttorie devono essere svolte nel rispetto dei principi di proporzionalità, minimizzazione dei dati, riservatezza, non discriminazione, presunzione di innocenza e tutela della persona coinvolta.

All'esito dell'istruttoria, il Gestore redige una relazione riservata contenente: oggetto della segnalazione, attività svolte, evidenze acquisite, valutazione di fondatezza, eventuali profili 231 o disciplinari, misure correttive proposte, eventuale necessità di coinvolgere autorità competenti e indicazioni di follow-up.

Il riscontro al segnalante deve essere fornito entro 3 mesi e può consistere nell'indicazione dell'archiviazione, dell'avvio o dello stato dell'istruttoria, delle misure adottate o programmate, nei limiti compatibili con la tutela della riservatezza, della persona coinvolta, del segreto aziendale e delle attività di indagine.

6. LA PROCEDURA DI SEGNALAZIONE ESTERNA TRAMITE ANAC

La segnalazione esterna è la comunicazione presentata attraverso il canale esterno gestito da ANAC. Essa è utilizzabile esclusivamente nei casi previsti dagli artt. 3 e 6 del D.Lgs. 24/2023 e non costituisce modalità alternativa libera rispetto al canale interno.

6.1. Condizioni per la segnalazione esterna

Nel perimetro in cui la segnalazione esterna è ammessa, è sufficiente una delle seguenti condizioni:

Il segnalante può ricorrere al canale esterno ANAC soltanto quando:

- il canale interno non è attivo o, anche se attivo, non è conforme alla normativa;
- la segnalazione interna già effettuata non ha avuto seguito nei termini previsti;
- il segnalante ha fondati motivi di ritenere che, effettuando una segnalazione interna, la stessa non avrebbe efficace seguito o esporrebbe il segnalante a rischio di ritorsioni;
- il segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Modalità e istruzioni aggiornate sono accessibili dalla pagina istituzionale ANAC https://www.anticorruzione.it/-/whistleblowing. Il segnalante segue le istruzioni ANAC per piattaforma, modalità orale o incontro diretto. Il Gestore interno non può subordinare l'accesso ad ANAC a una propria autorizzazione.

7. LA SEGNALAZIONE TRAMITE DIVULGAZIONE PUBBLICA E DENUNCIA

La divulgazione pubblica consiste nella comunicazione al pubblico di informazioni sulle violazioni tramite stampa, mezzi elettronici, social network o altri strumenti idonei a raggiungere un numero elevato di persone. Essa è ammessa solo al ricorrere delle condizioni tassative previste dalla legge.
Nei limiti dell'ambito di applicazione del decreto, la tutela nella divulgazione pubblica opera quando: a) sono state effettuate una segnalazione interna e una esterna, oppure direttamente una esterna nei casi consentiti, senza riscontro nei termini su misure previste o adottate; b) sussiste fondato motivo di ritenere un pericolo imminente o palese per il pubblico interesse; c) sussiste fondato motivo di ritenere che la segnalazione esterna comporti rischio di ritorsione o non abbia efficace seguito per le specifiche circostanze, quali occultamento o distruzione di prove, collusione o coinvolgimento dell'autorità destinataria. Il mero invio interno rimasto senza riscontro non basta, da solo, per la condizione sub a). Resta ferma la facoltà dei soggetti tutelati di presentare denuncia all'autorità giudiziaria o contabile per condotte illecite di cui siano venuti

a conoscenza nel contesto lavorativo. La presentazione della denuncia non esclude, ove ne ricorrano i presupposti, l'applicazione delle tutele previste dal D.Lgs. 24/2023.

8. IL REGIME DI PROTEZIONE PER I SEGNALANTI

La disciplina del whistleblowing prevede alcune importanti tutele a favore dei soggetti che segnalano le violazioni di illeciti e ai c.d. facilitatori, quali:

- Divieto di atti ritorsivi verso il segnalante;
- Nullità degli atti ritorsivi eventualmente compiuti;
- Riservatezza dell'identità del segnalante.

Tuttavia, il decreto 24/2023 prevede alcune condizioni che devono sussistere affinché il segnalante possa beneficiare del regime di protezione:

- Il segnalante deve essere un soggetto compreso nell'elenco dell'articolo 3 del d.lgs. 24/2023;
- Le violazioni segnalate o denunciate devono rientrare nell'ambito di applicazione del decreto;
- Il segnalante, al momento della segnalazione o denuncia, aveva fondato motivo di ritenere veritiere le informazioni;
- La segnalazione deve essere effettuata secondo le procedure previste dai canali interni ed esterni;
- La divulgazione pubblica deve essere stata effettuata alle condizioni previste dalla normativa.

Al contrario, il segnalante perde la protezione:

- Qualora sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di diffamazione o calunnia;
- In caso di responsabilità civile del segnalante per lo stesso titolo per dolo o colpa grave.

In entrambe le ipotesi verrà irrogata al segnalante una sanzione disciplinare.

8.1. Il divieto di ritorsioni e l'onere della prova

È vietata qualsiasi ritorsione, anche solo tentata o minacciata, collegata alla segnalazione.

Tra le possibili ritorsioni si considerano, a titolo esemplificativo:

- Licenziamento, sospensione o misure equivalenti;
- Retrocessione di grado o mancata promozione;
- Mutamento di funzioni, cambiamento del luogo di lavoro, riduzione dello stipendio, modifica degli orari di lavoro;
- Sospensione della formazione o restrizioni dell'accesso alla stessa;
- Note di merito negative o referenze negative;
- Adozione di misure disciplinari o altra sanzione, anche pecuniaria;

- Coercizione, intimidazione, molestie od ostracismo;
- Discriminazione o altri trattamenti sfavorevoli;
- Mancata conversione del contratto di lavoro a termine in contratto a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa alla conversione;
- Mancato rinnovo o risoluzione anticipata del contratto a termine;
- Danni, anche alla persona, in particolare sui social media o pregiudizi economici o finanziari, compreso la perdita di opportunità economiche e di redditi;
- Inserimento in elenchi impropri sulla base di accordo settoriale o industriale formale o informale;
- Conclusione anticipata o annullamento del contratto di fornitura di beni o servizi;
- Annullamento di una licenza o di un permesso;
- Richiesta di sottoposizione ad accertamenti psichiatrici o medici.

La tutela processuale, in questo caso, si sostanzia nell'inversione dell'onere della prova a carico del datore di lavoro. È quest'ultimo, dunque, che, in caso di procedimenti giudiziari, amministrativi o di controversie stragiudiziali che hanno ad oggetto l'accertamento delle ritorsioni subite dal segnalante, dovrà provare che tali atti sono motivati da ragioni estranee alla segnalazione. In caso contrario, vi è la presunzione che questi atti siano stati compiuti a causa della segnalazione e, pertanto, verranno considerati nulli.

Tale inversione dell'onere della prova non è prevista con riferimento ai segnalanti che non rientrano nell'ambito di un contesto prevalentemente lavorativo.

8.2. Protezione dalle ritorsioni e ruolo di ANAC

L'articolo 19 del d.lgs. 24/2023 stabilisce che il segnalante possa comunicare le misure ritorsive che ritiene di aver subito all'ANAC, la quale:

- In caso di ritorsioni commesse in ambito lavorativo pubblico, informa immediatamente il Dipartimento della funzione pubblica ed eventuali organismi di garanzia e disciplina;
- In caso di ritorsioni commesse in ambito lavorativo privato, informa l'Ispettorato nazionale del lavoro.

Se la procedura di verifica ha dato esito positivo, gli atti ritorsivi sono considerati nulli. Inoltre, l'autorità giudiziaria competente è tenuta ad adottare tutte le misure necessarie per assicurare la tutela della posizione giuridica del segnalante (risarcimento del danno, reintegrazione nel posto di lavoro, ordine di cessazione delle condotte ritorsive e nullità degli atti posti in essere).

8.3. Riservatezza e relativi limiti

Ai sensi dell'articolo 12 del d.lgs. 24/2023, il Gestore ha il dovere di garantire la **riservatezza del soggetto segnalante** sin dal momento della presa in carico della segnalazione, anche nelle ipotesi in cui la stessa dovesse rivelarsi successivamente errata o infondata.

In particolare, la Società deve garantire che l'identità del segnalante non possa essere rivelata senza il suo espresso consenso e tutti coloro che sono coinvolti nella gestione della segnalazione sono tenuti a tutelarne la riservatezza ad eccezione dei casi in cui:

- la segnalazione risulti fatta allo scopo di danneggiare o altrimenti recare pregiudizio al segnalato (c.d. segnalazione in "mala fede") e si configuri una responsabilità a titolo di calunnia o di diffamazione ai sensi di legge;
- la riservatezza non sia opponibile per legge (es. indagini penali).

Per quanto concerne, in particolare, l'ambito del procedimento disciplinare, **l'identità del segnalante non può essere rivelata**, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti ed 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 del segnalante sia indispensabile per la difesa dell'incolpato, **la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità**.

Tuttavia, le segnalazioni inviate allo scopo di danneggiare o altrimenti recare pregiudizio al segnalato nonché ogni altra forma di abuso **sono fonte di responsabilità del segnalante**, in sede disciplinare e nelle altre sedi competenti, in particolar modo se venga accertata la infondatezza di quanto segnalato e la strumentale e volontaria falsità di accuse.

A tal fine, qualora nel corso delle verifiche la segnalazione ricevuta si riveli intenzionalmente diffamatoria nonché la segnalazione si riveli infondata ed effettuata con dolo o colpa grave, in coerenza con quanto sopra descritto, la Società potrà applicare gli opportuni provvedimenti disciplinari.

8.4. Tutela della persona coinvolta

La Società garantisce la riservatezza e la dignità delle persone coinvolte o menzionate nella segnalazione, evitando la diffusione non necessaria di informazioni e assicurando che le verifiche siano svolte con imparzialità, proporzionalità e rispetto della presunzione di innocenza.
Il segnalato non ha diritto di conoscere l'identità del segnalante, salvo i casi previsti dalla legge. L'eventuale informativa alla persona coinvolta può essere ritardata o limitata quando ciò sia necessario per non pregiudicare la verifica della fondatezza della segnalazione, la raccolta delle prove, la riservatezza del segnalante o le attività delle autorità competenti.
La persona coinvolta può essere sentita e, su sua richiesta, è sentita anche mediante osservazioni scritte e documenti, secondo l'art. 12, comma 9. Nessuna misura sfavorevole si fonda sulla sola esistenza di una segnalazione, senza le necessarie verifiche e garanzie procedimentali.

9. LA CONSERVAZIONE DELLA DOCUMENTAZIONE

Segnalazioni e documentazione sono conservate per il tempo necessario al trattamento e comunque non oltre 5 anni dalla comunicazione dell'esito finale, ai sensi dell'art. 14 del D.Lgs. 24/2023. Alla scadenza il Gestore dispone cancellazione o distruzione sicura e ne documenta l'esecuzione. Eventuali atti necessari in un distinto procedimento giudiziario sono trattati separatamente sulla relativa base giuridica; non è ammessa una proroga indifferenziata dell'intero archivio whistleblowing.
Le segnalazioni ricevute tramite piattaforma sono conservate nell'archivio informatico del sistema, protetto da misure di crittografia, restrizione degli accessi e tracciabilità. Le segnalazioni

cartacee sono conservate in archivio fisico riservato, accessibile esclusivamente al Gestore o ai soggetti autorizzati per ragioni documentate.
Le segnalazioni orali, se registrate previo consenso, sono conservate su dispositivi idonei alla conservazione e all'ascolto. In caso di trascrizione o verbale, il segnalante deve poter verificare, rettificare e confermare il contenuto mediante sottoscrizione o altra modalità equivalente.
In caso di sostituzione del Gestore, il passaggio di consegne deve essere formalizzato mediante verbale riservato, contenente l'elenco dei fascicoli aperti e chiusi, lo stato delle istruttorie, le misure adottate e il monitoraggio dell'assenza di ritorsioni, garantendo la continuità delle misure di protezione e riservatezza.

10. IL TRATTAMENTO DEI DATI

Il Trattamento dei dati personali inerenti il Sistema di Gestione del Whistleblowing avviene nel rispetto del Regolamento (UE) 2016/679 (GDPR), nonché di eventuali altre leggi e/o regolamenti applicabili e compatibili e dell'informativa pubblicata sul sito internet della società (all' indirizzo **www.sidersipe.it** - di seguito "Informativa").

La gestione delle segnalazioni implica quanto meno il trattamento dei dati personali del segnalante (ove la segnalazione sia nominativa), del soggetto segnalato (ad esempio: nome, cognome, posizione ricoperta, ecc.), di eventuali terzi soggetti, nonché ogni ulteriore informazione raccolta nel contesto delle indagini necessaria ad accertare la fondatezza della segnalazione. I dati raccolti sono utilizzati in via esclusiva per il trattamento della segnalazione e quelli non utili allo scopo vengono immediatamente eliminati.

Il processo di gestione delle segnalazioni è improntato sul principio di *"garanzia di riservatezza e anonimato"* e il *"principio di riservatezza del Segnalante"* e, pertanto, nelle more del processo interno di accertamento, è garantita la massima riservatezza.

Qualora previsto dalle applicabili disposizioni di legge, gli interessati possono esercitare i diritti previsti dal GDPR inviando una comunicazione per posta elettronica all'indirizzo Titolare del Trattamento dei Dati, SIDER SIPE S.p.A.: **info@sidersipe.it**

Viene inoltre garantito il diritto di rivolgersi all'autorità per la protezione dei dati, competente in materia di trattamento illecito dei dati.

È sempre tutelata la riservatezza del Segnalante, la cui identità non può essere rivelata al Segnalato salvo i casi previsti dalla legge, al fine di evitare ritorsioni, minacce, violenze, discriminazioni ecc. dirette o indirette nei suoi confronti per motivi collegati, direttamente o indirettamente alla segnalazione. Tale principio non è garantito nel caso di segnalazione illecita.

La Società si riserva la facoltà di limitare o ritardare l'esercizio di detti diritti, conformemente a quanto stabilito dalle applicabili disposizioni di legge, nel caso in cui possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante e la compromissione della possibilità di verificare la fondatezza della segnalazione e/o di individuare le prove. In nessuna circostanza il segnalato, o terzi soggetti, potranno esercitare i propri diritti di accesso per ottenere informazioni sull'identità del segnalante, salvo che quest'ultimo abbia effettuato una segnalazione illecita.

La Società si riserva la facoltà di valutare le specifiche circostanze e condizioni che rendano opportuna una specifica informativa al segnalato sulla conclusione del procedimento, al fine di evitare ogni abuso e garantirne la tutela in qualità di interessato al trattamento dati.

11. IL SISTEMA SANZIONATORIO

La violazione della presente procedura, degli obblighi di riservatezza, del divieto di ritorsione, delle prescrizioni sui canali interni e dei doveri di collaborazione costituisce illecito disciplinare ed è sanzionata secondo il sistema disciplinare aziendale, il CCNL applicabile, il Modello 231 e la normativa vigente.

11.1. Le sanzioni previste da ANAC

L'articolo 21 del d.lgs. 24/2023 prevede alcune sanzioni amministrative pecuniarie che l'ANAC può applicare ai soggetti, sia pubblici che privati, che abbiano violato le regole stabilite dal d. lgs. 24/2023. In particolare:

- Sanzione da 10.000 a 50.000 euro in caso di condotte ritorsive, condotte ostative all'accertamento della segnalazione, violazione dell'obbligo di riservatezza;
- Sanzione da 10.000 a 50.000 euro in caso di mancata istituzione dei canali di segnalazione, mancata adozione delle procedure per la gestione delle segnalazioni o non conformità di queste alle prescrizioni degli articoli 4 e 5 del decreto;
- Sanzione da 500 a 2500 euro nei confronti del segnalante, in caso di accertamento della sua responsabilità per i reati di diffamazione o calunnia a titolo di dolo o colpa grave, salvo che via sia già stata condanna per i medesimi reati.

11.2. Sanzioni prevista da Sider Sipe S.p.A.

Ferma restando l'esclusiva competenza di ANAC in merito all'eventuale applicazione delle sanzioni amministrative di cui all'art. 21 del d.lgs. n. 24/2023, Sider Sipe S.p.A. assume adeguati provvedimenti disciplinari nei confronti:

- del Gestore delle Segnalazioni che non adempia agli obblighi previsti dalla presente procedura;
- di chi si renda responsabile di qualsivoglia atto di ritorsione o discriminatorio o comunque di pregiudizio illegittimo, diretto o indiretto, nei confronti del segnalante (e/o di chiunque abbia collaborato all'accertamento dei fatti oggetto di una segnalazione e/o dei soggetti connessi al segnalante) per motivi collegati, direttamente o indirettamente, alla segnalazione;
- del segnalato, per le responsabilità accertate;
- di chiunque violi gli obblighi di riservatezza richiamati dalla presente Procedura;
- di coloro, come previsto dalla legge, che abbiano effettuato una segnalazione infondata con dolo o colpa grave;
- di chi abusi dello strumento della segnalazione, come ad esempio effettuazione di segnalazioni con finalità opportunistiche e/o allo scopo di danneggiare l'accusato.

Si rinvia alla specifica disciplina prevista dal **Sistema Disciplinare del Modello Organizzativo 231** adottato da Sider Sipe S.p.A. per eventuali conseguenze sul piano disciplinare, nonché alla normativa giuslavoristica e contrattuale applicabile.

12. COORDINAMENTO CON MODELLO 231, ODV E FLUSSI INFORMATIVI

Il Sistema di Gestione del Whistleblowing costituisce presidio rilevante del sistema di controllo interno in coordinamento con le disposizioni del Modello 231.

In proposito, quando la segnalazione riguarda condotte rilevanti ai sensi del D.Lgs. 231/2001 o violazioni del Modello 231, il Gestore, qualora non coincida con l'OdV, informa tempestivamente quest'ultimo e valuta, comunque, l'apertura dell'istruttoria secondo le regole del presente Sistema.

Le risultanze anonime e aggregate delle segnalazioni, nonché le criticità ricorrenti emerse, sono utilizzate per aggiornare la mappatura dei rischi 231, i protocolli di controllo, il Codice Etico, la formazione e il sistema disciplinare.

13. FORMAZIONE, INFORMAZIONE, REPORTING E MONITORAGGIO

La Società assicura attività di formazione e informazione adeguate e periodiche, in modo da garantire una gestione consapevole, accurata e professionale delle segnalazioni al fine di diffondere una cultura di integrità e responsabilità.

La formazione del Gestore e dei soggetti autorizzati alla gestione del canale deve riguardare almeno: quadro normativo, presupposti delle segnalazioni, gestione istruttoria, comunicazioni con il segnalante, riservatezza, protezione da ritorsioni, trattamento dei dati personali, uso della piattaforma e gestione dei conflitti di interessi.

È opportuno prevedere formazione o informazione anche per tutto il personale, con esempi concreti di segnalazioni ammissibili e non ammissibili, istruzioni sull'uso del canale, tutele riconosciute, divieto di ritorsione e conseguenze degli abusi. La formazione deve essere aggiornata in occasione di modifiche normative, aggiornamenti del canale o revisioni della procedura.

Le informazioni sul canale interno, sulle procedure e sui presupposti per le segnalazioni interne ed esterne devono essere chiare, facilmente accessibili e diffuse attraverso: pubblicazione sul sito aziendale, intranet o bacheche, consegna o comunicazione al personale, informativa a fornitori, consulenti, collaboratori e partner commerciali, nonché richiamo nei contratti o documenti di *onboarding*, ove pertinente.

Con frequenza almeno annuale, il Gestore redige una relazione riservata sulle segnalazioni ricevute, archiviate e oggetto di istruttoria, sulle tipologie di violazioni, sulle misure adottate, sulle eventuali criticità del Sistema e sulle proposte di aggiornamento. La relazione è trasmessa agli organi di amministrazione e controllo competenti, in forma tale da non rivelare l'identità del segnalante o informazioni non necessarie.