ROHDE & SCHWARZ ITALIA SPA

REGOLAMENTO WHISTLEBLOWING

Prima redazione dicembre 2023
approvato in data 15/12/2023
Seconda Revisione Luglio 2025
approvato in data 11/07/2025
Terza Revisione Luglio 2026
Approvato in data 31/07/2026

_____

Sommario

1 GLOSSARIO 4
2 PREMESSA 5
2.1 Obiettivi del documento 5
2.2 Adozione, aggiornamento e diffusione del documento 6
2.3 Contesto normativo di riferimento 7
2.4 Perimetro di applicazione 7
2.4.1 Enti soggetti alla normativa 7
2.4.2 Segnalante 8
2.4.3 Violazioni 8
2.5 Tutela e garanzie per i soggetti coinvolti 10
2.5.1 Divieto di ritorsioni 11
2.5.2 Misure di tutela 11
2.6 Confronto con le parti sociali 11
3 RUOLI E RESPONSABILITÀ DI RSI 12
3.1 Consiglio di Amministrazione 12
3.2 Organismo di Vigilanza 231 ("OdV") 12
3.3 Compliance Manager 13
3.4 Collegio Sindacale 13
3.5 Presidente del Consiglio di Amministrazione 13
3.6 Vicepresidente del Consiglio di Amministrazione 13
3.7 Presidente del Collegio Sindacale 13
3.8 Sindaco più anziano 14
3.9 Struttura che si occupa della gestione del personale (5SEU HR Management) 14
3.10 Struttura che si occupa dei rapporti con terzi (Marketing & Communications) 14
4 INFORMAZIONE E FORMAZIONE 14
5 PROCEDURA INFORMATICA 15
5.1 Canali di segnalazione interni per Whistleblowing 15
5.1.1 Canali di segnalazione standard "Corporate" 15
5.1.2 Canale di segnalazione informatico Whistleblowing "Corporate" 15
5.1.3 Canale interno RSI in modalità vocale 15
5.2 Canale di segnalazione esterno per Whistleblowing 15
6 SEGNALAZIONI (POTENZIALI) DELLE VIOLAZIONI 16
6.1 Processo di gestione delle segnalazioni 16
6.1.1 Inserimento e invio della segnalazione 17
6.1.2 Ricezione, esame e valutazione 18
6.1.3 Definizione delle misure di intervento 20
6.2 Archiviazione della documentazione 21
6.3 Registro 22
6.4 Relazione annuale 22

7 PRESIDI DI CONTROLLO 22

1 GLOSSARIO

Capogruppo: Rohde & Schwarz GmbH & Co. KG, in qualità di capogruppo *Corporate*, con sede a Monaco di Baviera (Germania).

Consiglio di Amministrazione (CdA): Organo con funzione di supervisione strategica della Rohde & Schwarz Italia SPA.

Contesto lavorativo: le attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di cui all'articolo 3, commi 3 o 4, del Decreto Legislativo 24/2023 attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria.

Esponente Aziendale: i soggetti che svolgono funzioni di amministrazione, direzione e controllo.

Facilitatore: 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.

Funzione investigante: struttura incaricata di svolgere le indagini sulle segnalazioni ricevute nei casi previsti dal presente Regolamento.

Gruppo Societario: le Società del gruppo *Corporate* e le altre società non strumentali controllate, direttamente e/o indirettamente, dalla Capogruppo.

Persona coinvolta: la persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.

Personale: personale dipendente e coloro che operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato (es.: contratti di somministrazione, collaboratori, stagisti ecc.).

Response Team: è un organismo centrale e indipendente gestito direttamente dalla Compliance Corporate R&S. Il Response Team è composto da tre membri del top management. Il responsabile del Response Team è altresì responsabile dei dipartimenti aziendali Legal Services, Compliance e Internal Audit. Il team è delegato direttamente dall'Executive Board per la responsabilità delle proprie funzioni.

Ritorsione: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria 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.

Riscontro: comunicazione alla persona segnalante di informazioni relative al seguito che viene dato o che si intende dare alla segnalazione.

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

Segnalato: il soggetto che viene ritenuto, dal Segnalante, responsabile di una violazione comunicata nell'ambito di una Segnalazione come di seguito definita.

Segnalazione: comunicazione relativa a comportamenti di qualsiasi natura (anche omissivi) seriamente sospetti di violazioni.

Seguito: l'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate.

Sistema di Whistleblowing Corporate: un sistema informatico per le segnalazioni Whistleblowing denominato “R&S Speak Up!” gestito dalla Compliance Corporate e realizzato per garantire un approccio olistico, aperto a tutte le filiali del gruppo, per il rispetto degli standard e la protezione del whistleblower.

Whistleblowing: è la segnalazione compiuta da un segnalante che, nello svolgimento delle proprie mansioni, viene a conoscenza di informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell’organizzazione con cui la persona segnalante intrattiene un rapporto giuridico, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni.

Violazioni: 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 numeri 3), 4), 5) e 6);
2) condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazioni dei modelli di organizzazione e gestione ivi previsti, che non rientrano nei numeri 3), 4), 5) e 6);
3) illeciti che rientrano nell’ambito di applicazione degli atti dell’Unione europea o nazionali indicati nell’allegato al presente decreto 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 presente decreto, 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;
4) 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;
5) 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;
6) 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).

2 PREMESSA

2.1 Obiettivi del documento

II Regolamento Whistleblowing (di seguito "Regolamento") di Rohde & Schwarz Italia SPA (d’ora in poi anche "RSI") ha l'obiettivo di fornire le linee guida da seguire per la segnalazione di atti o fatti che

possano costituire una violazione delle norme, interne ed esterne, disciplinanti:

- l'attività commerciale, di progettazione, installativa o di assistenza tecnica, incluse le relative attività connesse e strumentali, la violazione ai principi e alle regole di comportamento contenute nel Codice Etico, le violazioni del Modello di Organizzazione e Gestione di RSI, i comportamenti illeciti o fraudolenti compiuti da dipendenti o esponenti aziendali e di violazioni durante lo svolgimento delle proprie mansioni professionali, nell'ottica di contribuire all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per RSI e, di riflesso, nell'interesse dell'intero gruppo *Corporate* e di tutti gli stakeholder, permettendo di agire efficacemente al riguardo, con particolare *focus* su:

- leggi sulla concorrenza e antitrust;
- corruzione/concussione/conflitto di interessi;
- frode/malversazione/furto/appropriazione indebita;
- controllo delle esportazioni, embarghi, sanzioni;
- protezione di dati/informazione e sicurezza informatica (*cybersecurity*);
- discriminazione/molestie/mobbing;
- standard ambientali e sociali, inclusa la sicurezza sul lavoro e i diritti umani (nella catena di fornitura);
- altra violazione delle leggi e/o delle policy interne.

- gli illeciti commessi in violazione della normativa dell'UE in una serie di settori identificati nell'Allegato 1 al Decreto legislativo n. 24/2023 (ad esempio in materia di tutela dell'ambiente; appalti pubblici; sicurezza dei trasporti; salute pubblica; ecc.) e di tutte le disposizioni nazionali che ne danno attuazione; gli atti od omissioni che ledono gli interessi finanziari dell'Unione Europea (art. 325 del TFUE lotto contra la frode e le attività illegali che ledono gli interessi finanziari dell'UE) come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE;
- gli atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali. Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposto sulle società e 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;
- gli atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea nei settori sopra indicati compiuti dai soggetti indicati nel paragrafo relativo al perimetro di applicazione.

II Regolamento fornisce, inoltre, le linee guida per garantire la riservatezza delle informazioni trasmesse, la protezione dei dati personali del soggetto che effettua la Segnalazione e del soggetto Segnalato e la tutela del Segnalante da eventuali condotte ritorsive, discriminatorie o comunque sleali conseguenti alla Segnalazione.

Le linee guida sono state progettate per essere coerenti con le normative aziendali e le descrizioni procedurali, al fine di garantire un approccio olistico a livello corporate.

2.2 Adozione, aggiornamento e diffusione del documento

II presente Regolamento, e i suoi relativi aggiornamenti, sono approvati dal Consiglio di

Amministrazione di RSI su proposta dell'Organismo di Vigilanza 231 ("OdV", in qualità di Responsabile dei Sistemi Interni di Segnalazione) e con il parere della Compliance Manager.

II Regolamento si applica alla Rohde & Schwarz Italia SpA la quale provvede all'aggiornamento del Regolamento qualora si verifichino cambiamenti rilevanti nella normativa di riferimento o nei propri assetti organizzativi.

2.3 Contesto normativo di riferimento

RSI opera nel pieno rispetto di tutte le leggi e regolamenti sovranazionali, nazionali e locali applicabili.

Le principali fonti normative esterne di riferimento sono identificate nell'elenco dei reati presupposto di cui al Modello di Organizzazione e di Gestione – parte generale di RSI, nonché, a titolo esplicativo e non esaustivo:

- Decreto Legislativo 8 giugno 2001, n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" e successive modifiche e integrazioni - art. 6 "Soggetti in posizione apicale e modelli di organizzazione dell'ente".
- Legge 30 novembre 2017, 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" e successive modifiche e integrazioni - art. 3 "Integrazione della disciplina dell'obbligo di segreto d'ufficio, aziendale, professionale, scientifico e industriale".
- Decreto Legislativo n. 24 del 10 marzo 2023, pubblicato in GU in data 15.03.2023 Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.
- Linee guida della Autorità Nazionale Anticorruzione in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne approvate con Delibera n. 311 del 12 luglio 2023.
- Guida operativa per gli enti privati di Confindustria su "*nuova disciplina "whistleblowing"*" di ottobre 2023.

Di seguito si riportano alcune delle principali fonti normative interne di riferimento:

- Codice Etico;
- Modello 231.

2.4 Perimetro di applicazione

2.4.1 Enti soggetti alla normativa

Per il **settore privato**, la **disciplina si applica alle seguenti categorie di soggetti**:

- enti che hanno impiegato, nell'ultimo anno, la media di **almeno cinquanta lavoratori** subordinati

con contratti di lavoro a tempo indeterminato o determinato;

- enti che rientrano nell'ambito di applicazione del decreto legislativo 8 giugno 2001, n. 231, e adottano Modelli di organizzazione e gestione ivi previsti, anche se nell'ultimo anno non hanno raggiunto la media di 50 lavoratori subordinati;
- enti che rientrano nell'ambito di applicazione degli atti dell'Unione di cui, alle parti I.B e II dell'allegato del Decreto, ovvero enti **soggetti alla normativa in materia di servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo, anche se nell'ultimo anno non hanno raggiunto la media di 50 lavoratori subordinati**.

2.4.2 Segnalante

Con il termine Segnalante si intendono tutti i soggetti che possono effettuare una Segnalazione.

Possono effettuare una Segnalazione tutte le **persone fisiche** che operano come:

- i lavoratori subordinati, ivi compresi i lavoratori il cui rapporto di lavoro è disciplinato dal decreto legislativo 15 giugno 2015, n. 81, o dall'articolo 54-bis del decreto-legge 24 aprile 2017, n. 50, convertito, con modificazioni, dalla legge 21 giugno 2017, n. 96;
- i lavoratori autonomi, ivi compresi quelli indicati al capo I della legge 22 maggio 2017, n. 81, nonché i titolari di un rapporto di collaborazione di cui all'articolo 409 del codice di procedura civile e all'articolo 2 del decreto legislativo n. 81 del 2015;
- i lavoratori o i collaboratori che forniscono beni o servizi o che realizzano opere in favore di terzi;
- i liberi professionisti e i consulenti;
- i volontari e i tirocinanti, retribuiti e non retribuiti;
- gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.

Tale possibilità viene riconosciuta anche quando uno dei rapporti giuridici sopra menzionati non è 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.

2.4.3 Violazioni

Le disposizioni contenute nel Regolamento **si applicano** a tutti i comportamenti, atti o omissioni che ledono l'interesse pubblico o dell'ente privato commesse nell'ambito dell'organizzazione dell'ente con cui il Segnalante intrattiene uno dei rapporti giuridici qualificati considerati dal Legislatore.

Ai fini del presente documento, si comunicano gli atti o i fatti che possono costituire:

- violazioni di norme interne ed esterne disciplinanti le attività di RSI, incluse le relative attività connesse o strumentali;
- violazione ai principi e alle regole di comportamento contenute nel Codice Etico;
- comportamenti illeciti o fraudolenti compiuti da dipendenti o esponenti aziendali, durante lo svolgimento delle proprie mansioni professionali, che possano determinare in modo diretto o indiretto, un danno economico-patrimoniale e/o di immagine per la Società. Tali atti o fatti sono riconducibili, a titolo esemplificativo ma non esaustivo, alle seguenti tipologie:

- furto, frode e appropriazione indebita;

- violazioni in materia di governo societario e politiche di remunerazione;
- violazioni in materia di trasparenza bancaria e finanziaria;
- illecito utilizzo di deleghe e poteri;
- elusione di regole e controlli contabili;
- rilascio consapevole di dati ed informazioni aziendali falsi o non corretti;
- attuazione di pratiche commerciali scorrette o ingannevoli;
- effettuazione di operazioni o altri comportamenti in violazione delle disposizioni in tema di *market abuse*;
- effettuazione di operazioni o altri comportamenti in violazione delle disposizioni sui conflitti di interesse:
- effettuazione di operazioni o altri comportamenti in violazione delle norme in materia di servizi di investimento;
- utilizzo improprio/irregolare di risorse aziendali a propria disposizione;
- trattamento non autorizzato/indebito di dati personali;
- violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo, o elusione degli obblighi normativi con riferimento a violazione di embarghi;

- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al presente decreto 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 presente decreto, 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; tutelo della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- 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;
- atti od omissioni riguardanti ii 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 ii 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;
- 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);
- normative interne in materia di *diversity and inclusion*.

Le disposizioni del Regolamento **non si applicano**:

- alle **contestazioni, rivendicazioni o richieste** legate ad un **interesse di carattere personale** della persona segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate;
- alle segnalazioni di violazioni in materia di **sicurezza nazionale**.

2.5 Tutela e garanzie per i soggetti coinvolti

La segnalazione è libera e spontanea, l'unico onere a carico del Segnalante riguarda l'obbligo di dichiarare se egli abbia un interesse personale collegato alla Segnalazione.

Vengono adottate misure volte ad assicurare, sin dalla ricezione della Segnalazione e in ogni fase successiva, la riservatezza dell'identità e la protezione dei dati personali del Segnalante, che si espone in prima persona segnalando un illecito, del Segnalato, degli eventuali altri soggetti eventualmente coinvolti nonché del contenuto della Segnalazione e della relativa documentazione[1].

Tutti i soggetti coinvolti nella gestione della Segnalazione sono tenuti a garantire la riservatezza e la protezione dei dati personali dei diversi soggetti coinvolti e del contenuto della Segnalazione insieme alla documentazione allegata, così come l'anonimato, esclusivamente nei casi previsti dalla normativa. La violazione degli obblighi di riservatezza è fonte di responsabilità disciplinare, fatto salvo ogni ulteriore forma di responsabilità prevista dalla legge.

II Gruppo assicura la riservatezza dell'identità del Segnalante, fatta eccezione nei casi in cui:

- il Segnalante esprime il suo consenso alla divulgazione;
- la sua divulgazione sia necessaria per le indagini o i procedimenti avviati dall' Autorità Giudiziaria in seguito alla Segnalazione o se e indispensabile per la difesa del segnalato.

Inoltre, la divulgazione non autorizzata dell'identità del Segnalante oppure di informazioni in base alle quali la stessa si possa dedurre, o qualsiasi azione finalizzata a svelare illegalmente l'identità del Segnalante, sono considerate una violazione del presente Regolamento ed è, come detto, fonte di responsabilità disciplinare, fatta salvo ogni ulteriore forma di responsabilità prevista dalla legge.

Al Segnalante non vengono garantite le tutele previste nel presente Regolamento qualora la Segnalazione riporti informazioni false, rese con dolo o colpa grave (c.d. Segnalazione in "mala fede"); tale comportamento. potrà dare luogo anche ad un procedimento disciplinare o azioni legali nei suoi confronti (Cfr. par. 6.1.3).

Al soggetto Segnalato, non sarà riconosciuto il diritto di ottenere l'indicazione dell'origine dei dati personali che lo riguardano, come previsto dall'art 2-undecies, comma l lettera f) del D.lgs. 101/2018 il quale stabilisce specifiche limitazioni ai diritti dell'interessato che non possono essere esercitati con richiesta al titolare o al responsabile del trattamento ovvero con reclamo, nel caso in cui da tale esercizio posso scaturire un pregiudizio concreto ad altri interessi superiori normativamente tutelati.

Sono garantite misure di protezione al Segnalante (**divieto di ritorsioni[2] e misure di sostegno**) nonché ai Facilitatori, alle persone che lavorano nello stesso contesto lavorativo del Segnalante, alle persone che hanno uno stabile legame affettivo o di parentela entro il quarto grado, ai colleghi di

---

[1] Si rappresenta che il divieto di rivelare l'identità del Segnalante è da riferirsi non solo al nominativo del Segnalante ma anche a qualsiasi altra informazione o elemento della Segnalazione, ivi inclusa la documentazione ad essa allegata, dal cui disvelamento si possa dedurre direttamente o indirettamente l'identità del Segnalante. Il trattamento di tutti questi elementi è quindi improntato alla massima cautela, a cominciare dall'oscuramento dei dati personali, specie quelli relativi al Segnalante ma anche degli altri soggetti la cui identità deve rimanere riservata (il Facilitatore, il Segnalato, le altre persone menzionate nella Segnalazione, qualora, per ragioni istruttorie, anche altri soggetti debbano essere messi a conoscenza del contenuto della Segnalazione e/o della documentazione ad essa allegato.

[2] La definizione di “ritorsione” contempla non solo le ipotesi in cui la ritorsione si sia già verificata, ma anche quelle in cui sia soltanto “tentata” oppure “minacciata”.

lavoro con i quali il Segnalante ha un rapporto abituale e corrente e agli enti di proprietà del segnalante.

2.5.1 Divieto di ritorsioni

II soggetto che effettua una Segnalazione o una segnalazione esterna o una divulgazione pubblica, nei casi previsti dalla normativa di riferimento, non può subire ritorsioni di alcun genere purché la stessa sia inoltrata in buona fede e ragionevolmente ritiene, anche alla luce delle circostanze del caso concreto e dei dati disponibili al momento della Segnalazione, che le informazioni sulle violazioni segnalate siano veritiere.

2.5.2 Misure di tutela

Le persone segnalanti beneficiano di misure di protezione a condizione che abbiano avuto fondati motivi di ritenere che le informazioni segnalate fossero vere al momento della Segnalazione e che tali informazioni rientrassero nell'ambito di applicazione della disciplina.

Si precisa inoltre che le misure di protezione si applicano anche:

- ai Facilitatori, ossia le persone fisiche che assistono il Segnalante nel processo di Segnalazione, e che operano all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata. A titolo esemplificativo, il Facilitatore potrebbe essere il collega di un ufficio diverso da quello di appartenenza del segnalante che assiste quest'ultimo nel processo di Segnalazione in via riservata, cioè senza divulgare le notizie apprese. II Facilitatore potrebbe essere un collega che riveste anche la qualifica di sindacalista se assiste il Segnalante in suo nome e per suo canto, senza spendere la sigla sindacale;
- alle persone del medesimo contesto lavorativo del Segnalante che operano, o hanno operato in passato, nel medesimo ambiente lavorativo della Persona segnalante (a titolo esemplificativo colleghi, ex-colleghi, Collaboratori), nonché ai terzi che sono legati al Segnalante da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro del Segnalante che lavorano nel medesimo contesto lavorativo e che hanno con detta persona un rapporto abituale e corrente;
- alle entità societarie del Segnalante o per le quali la stessa persona lavora, nonché entità che operano nel medesimo contesto lavorativo delle già menzionate persone.

I canali interni di segnalazione devono poter garantire il rispetto degli **obblighi di riservatezza**:

- dell'identità del Segnalante;
- dell'identità del Segnalato;
- del contenuto della Segnalazione e della relativa documentazione allegata.

2.6 Confronto con le parti sociali

Le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, sono preventivamente sentite in merito ai canali interni di segnalazione attivati dalla Società, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella Segnalazione, nonché del contenuto della Segnalazione e della relativa documentazione.

3 RUOLI E RESPONSABILITÀ DI RSI

Di seguito si riporta il dettaglio, in termini di ruoli e responsabilità, degli Organi e delle Strutture di Rohde & Schwarz Italia SPA coinvolti nel presidio del processo correlato alla Segnalazione.

3.1 Consiglio di Amministrazione

II Consiglio di Amministrazione, nella sua qualità di Organo con funzione di supervisione strategica:

- avalla, su proposta dell'OdV (in qualità di Responsabile dei Sistemi Interni di Segnalazione) e con il parere della Compliance Manager ed in seguito ad approvazione da parte dell'Amministratore Delegato, il presente Regolamento e i successivi aggiornamenti;
- nomina i membri dell'OdV;
- attiva un canale di segnalazione che garantisca, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità del Segnalante, della persona coinvolta e della persona comunque menzionata nella Segnalazione, nonché del contenuto della Segnalazione e della relativa documentazione:
- adotta procedure per l'effettuazione e la gestione delle segnalazioni conformi a quanto previsto dalla normativa di riferimento;
- assicura nel continuo che compiti e responsabilità siano allocati in modo chiaro ed appropriato, garantendo la chiara distinzione di incarichi e funzioni, la prevenzione di potenziali conflitti di interesse e un sistema idoneo a garantire la corretta gestione delle Segnalazioni e delle tutele e garanzie per i soggetti coinvolti;
- con cadenza annuale, viene informato sulle risultanze dell'attività svolta da RSI in relazione alle segnalazioni da loro ricevute, attraverso la relazione predisposta dall'OdV e redatta anche sulla base delle informazioni trasmesse dalla Capogruppo;
- supervisiona ii processo di formazione ai dipendenti e di informazione a tutto il Personale;
- definisce i provvedimenti necessari da adottare secondo quanto previsto dal presente documento (Cfr. par. 6.1.3), dandone informativa all'OdV.

3.2 Organismo di Vigilanza 231 ("OdV")

In qualità di Responsabile dei Sistemi Interni di Segnalazione:

- riceve e gestisce la Segnalazione in base a quanto previsto dal presente documento (Cfr. par. 6.1.2) per il tramite della procedura informatica adottata da RSI e nel rispetto dei principi di riservatezza, mantiene i rapporti con il Segnalante sulla presa in carico della Segnalazione, sull'eventuale richiesta di dati e informazioni aggiuntive e sulla comunicazione dell'esito della stessa;
- con il supporto delle strutture competenti, mette a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne ed esterne. Le suddette informazioni sono esposte e rese facilmente visibili attraverso la pubblicazione in una sezione

dedicata del sito internet di RSI;

- riferisce, direttamente e senza indugio, al Consiglio di Amministrazione e al Collegio Sindacale le Segnalazioni di particolare gravità;
- redige una relazione annuale sul corretto funzionamento dei Sistemi Interni di segnalazione, contenente, in forma anonima, le informazioni aggregate sui casi, la numerosità delle indagini svolte e le tipologie dei provvedimenti adottati a seguito delle Segnalazioni ricevute;
- successivamente alla presa d'atto della relazione annuale da parte del Consiglio di Amministrazione e dal Collegio Sindacale, mette la stessa a disposizione del Personale.

In qualità di Organismo di Vigilanza 231:

- tratta le Segnalazioni ogni qualvolta la presunta violazione abbia un impatto anche con riferimento agli illeciti previsti dal S. Lgs. 231/2001, tale da prefigurare l'eventuale coinvolgimento della Società per illecito amministrativo;
- valuta se la Segnalazioni possono avere degli impatti anche sul Modello di Organizzazione e Gestione adottato ai sensi del D. Lgs. 231/2001.

3.3 Compliance Manager

Il Compliance Manager fornisce al Consiglio di Amministrazione il proprio parere di conformità in merito all'adozione e all'aggiornamento del presente Regolamento.

3.4 Collegio Sindacale

II Collegio Sindacale con cadenza annuale prende atto della relazione predisposta dall'OdV (in qualità di Responsabile dei Sistemi Interni di Segnalazione), redatta sulla base delle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, anche sulla base delle informazioni trasmesse dalla Capogruppo.

3.5 Presidente del Consiglio di Amministrazione

Per assicurare che ii soggetto preposto alla ricezione della Segnalazione non sia gerarchicamente o funzionalmente subordinato all'eventuale soggetto Segnalato, non sia esso stesso ii presunto responsabile della violazione e non abbia un potenziale interesse correlato alla Segnalazione tale da compromettere l'imparzialità e l'indipendenza del giudizio, è attribuita al Presidente del Consiglio di Amministrazione la responsabilità di gestire le segnalazioni che identificano come presunto responsabile della violazione il Presidente e/o membri del Collegio Sindacale (canale alternativo).

3.6 Vicepresidente del Consiglio di Amministrazione

Al Vicepresidente del Consiglio di Amministrazione è attribuito il compito di gestire le segnalazioni indirizzate al Presidente del Consiglio di Amministrazione in caso di sua assenza improvvisa/prolungata.

3.7 Presidente del Collegio Sindacale

Per assicurare che il soggetto preposto alla ricezione non sia gerarchicamente o funzionalmente

subordinato all'eventuale soggetto Segnalato, non sia esso stesso il presunto responsabile della violazione e non abbia un potenziale interesse correlato alla Segnalazione tale da compromettere l'imparzialità e l'indipendenza del giudizio, è attribuito al Presidente del Collegio Sindacale la responsabilità di gestire le segnalazioni che identificano come presunti responsabili della violazione gli Esponenti aziendali (Amministratore Delegato, Direzione Generale, Consiglio di Amministrazione) o l'OdV/Responsabile dei Sistemi interni di Segnalazione e i suoi collaboratori.

3.8 Sindaco più anziano

AI Sindaco effettivo più anziano è attribuito il compito di gestire le segnalazioni indirizzate al Presidente del Collegio Sindacale in caso di sua assenza improvvisa/prolungata.

3.9 Struttura che si occupa della gestione del personale (5SEU HR Management)

La Direzione Risorse Umane assicura che il presente documento dia portato a conoscenza e disponibile per la consultazione da tutto il Personale.

Organizza iniziative di comunicazione interna e di formazione sul funzionamento dei Sistemi interni di Segnalazione adottato dal Gruppo, indicando i presidi posti a garanzia della riservatezza dei dati personali, gli strumenti e le procedure da seguire per la gestione della Segnalazione in tutte le sue fasi, dall'inserimento fino alla conclusione.

Può altresì supportare gli Organi aziendali competenti nella definizione e gestione delle eventuali misure di intervento (Cfr. Par. 6.1.3).

3.10 Struttura che si occupa dei rapporti con terzi (Marketing & Communications)

La struttura che si occupa dei rapporti con terzi (o sito internet) supporta l'OdV (in qualità di Responsabile dei sistemi interni di Segnalazione) circa la messa a disposizione delle informazioni necessarie in materia (Cfr. 3.2, secondo punto).

4 INFORMAZIONE E FORMAZIONE

La Corporate Compliance, come titolare del processo a livello di gruppo, svolge regolarmente la formazione per i membri del sistema di compliance di gruppo e comunica regolarmente a tutto il gruppo aziendale sulla presente materia attraverso il Sistema di Whistleblowing Corporate.

RSI organizza iniziative di comunicazione interna e verso l'esterno indicando i presidi posti a garanzia della riservatezza dei dati personali (sia del Segnalante, del Segnalato che di tutti gli elementi contenuti nella Segnalazione), i canali per effettuare le segnalazioni e le procedure da seguire per la gestione della Segnalazione in tutte le sue fasi, dall'inoltro fino alla conclusione.

Sono inoltre organizzate iniziative di formazione agli Esponenti Aziendali ed al Personale sul funzionamento del Sistema interno di Segnalazione adottato.

5 CANALI DI SEGNALAZIONE

Il sistema di segnalazione Whistleblowing Corporate dispone di diversi possibili canali di segnalazione, che include le seguenti procedure.

5.1 Canali di segnalazione interni per Whistleblowing

5.1.1 Canali di segnalazione standard “Corporate”

I canali di segnalazione “Corporate” includono la possibilità di contatto confidenziale tramite e-mail “Corporate” (compliance@rohde-schwarz.com), riferimento telefonico (+49 89 41 29-12 500) oppure di persona (diretto contatto dei Compliance Corporate Officers.

5.1.2 Canale di segnalazione informatico Whistleblowing “Corporate”

La Compliance Corporate prevede l’utilizzo di uno strumento informatico di Whistleblowing denominato “R&S Speak Up!”, che può essere utilizzato in modalità completamente anonima, che archivia i dati in forma criptata e protetta. Questo canale è disponibile e aperto anche per terze parti, è raggiungibile sul sito ufficiale Rohde & Schwarz cliccando sul link: “R&S Speak Up!”. La procedura consente di inserire la segnalazione garantendo sempre l'assoluta riservatezza dei dati del Segnalante, la confidenzialità delle informazioni fornite dallo stesso e l'anonimato nei casi previsti dalla normativa di riferimento. Una volta inoltrata la Segnalazione tramite la procedura messa a disposizione, il Segnalante ha la possibilità di verificare in qualsiasi momento, accedendo nuovamente alla procedura, la conferma di ricezione della Segnalazione, lo stato di avanzamento della pratica e le eventuali richieste di approfondimenti e/o di ulteriore documentazione a supporto.

L'Archivio delle segnalazioni garantisce la tracciabilità e l'archiviazione dei dati permettendo alle strutture preposte di predisporre una reportistica dettagliata e strutturata, garantendo la riservatezza o l'anonimato dei dati contenuti nelle singole pratiche.

Le misure di sicurezza adottate dovranno essere costantemente testate e verificate secondo l'evoluzione della tecnologia e delle best practice di sicurezza sottoponendole a controllo periodico per accertare la loro idoneità a garantire un presidio efficace dei rischi per i diritti e le libertà dell'individuo.

5.1.3 Canale interno RSI in modalità vocale

Casella vocale raggiungibile al numero telefonico **06 41598 335**

La casella vocale è configurata sulla centrale telefonica (PBX) di RSI. Nel caso in cui si voglia nascondere il proprio numero di telefono, utilizzare la relativa opzione (p.es. anteponendo il codice: #31#), in modo da garantire la necessaria riservatezza.

L’evidenza della presenza di un messaggio è data da un’apposita segnalazione sull’apparecchio telefonico messo a disposizione dell’OdV.

L’accesso ai messaggi vocali registrati è possibile solo attraverso apposito PIN, conosciuto solo dall’OdV stesso, per poter garantire la necessaria riservatezza.

5.2 Canale di segnalazione esterno per Whistleblowing

Sul sito internet di Rohde & Schwarz Italia SPA, raggiungibile all’URL http://www.rohde-schwarz.it,

è stato predisposto un apposito link verso il sistema di segnalazione dell'Autorità Nazionale Anti Corruzione (ANAC): https://www.anticorruzione.it/-/whistleblowing.

Ciascun segnalante potrà eventualmente inserire la propria segnalazione, nel caso in cui, ad esempio, il canale interno non risulti efficace, oppure nel caso il segnalante ritenga che ci sia un pericolo imminente per la Società.

Si ricorda che è altresì prevista la possibilità della c.d. "divulgazione pubblica" (a cui si può ricorrere, però, **solo se è già stata effettuata la segnalazione verso il canale interno** o verso l'ANAC, oppure in caso di pericolo imminente, ovvero di ritorsione).

6 SEGNALAZIONI DELLE VIOLAZIONI (POTENZIALI)

La capogruppo ha sviluppato una descrizione del processo (relativo alla gestione delle segnalazioni) con principi procedurali chiari, accessibile in modo trasparente a tutti i dipendenti. Il processo prevede che la Corporate Compliance, in qualità di garante del processo e organismo di riferimento, verifichi la plausibilità generale di ogni segnalazione in entrata (digitale o analogica). Le segnalazioni palesemente irrilevanti o non pertinenti alla compliance vengono automaticamente archiviate in questa fase. Se la segnalazione viene ritenuta plausibile, il Response Team, composto da tre membri del top management, stabilisce i passi successivi. Qualora vi sia un collegamento con il Sistema di Segnalazione Interna (RSI), la questione viene delegata in modo appropriato e diretto all'organo competente, l'Organismo di Vigilanza D.Lgs. 231/2001, per la revisione e l'elaborazione a livello locale. RSI riceverà quindi un accesso separato al sistema informatico di segnalazione per poter gestire la questione in modo indipendente e locale all'interno del sistema. La Compliance Corporate, in qualità di garante del Sistema di Segnalazione Interna Corporate, supervisiona l'intero processo sulla base di principi procedurali ed è a disposizione dell'Organismo di Vigilanza D.Lgs. 231/2001 per fornire supporto qualificato in qualsiasi momento.

6.1 Processo di gestione delle segnalazioni

Nell'ambito della gestione del canale di segnalazione interna, la Compliance Corporate e/o il Response Team oppure, a seconda del caso, l'OdV (in qualità di Responsabile dei Sistemi Interni di Segnalazione) svolge le seguenti attività:

a) rilascia alla persona segnalante un avviso di ricevimento della segnalazione entro **sette giorni** dalla data di ricezione;
b) mantiene le interlocuzioni con il Segnalante e può richiedere a quest'ultimo, se necessario, integrazioni rispetto al contenuto della segnalazione;
c) dà seguito alle segnalazioni ricevute in base a quanto stabilito dal presente Regolamento;
d) fornisce riscontro alla segnalazione entro **novanta giorni** dalla data dell'avviso di ricevimento, in mancanza di tale avviso, entro **novanta giorni** o alla scadenza del termine di **sette giorni** dalla presentazione della segnalazione;

Alle segnalazioni inoltrate in forma anonima e riferite all'ambito antiriciclaggio, non si applicano i precedenti punti a), b) e d).

La Segnalazione deve fornire tutti gli elementi utili per consentire un'appropriata attività di riscontro della sua fondatezza e delle eventuali violazioni. Tali segnalazioni sono raccolte attraverso un'apposita procedura informatica di whistleblowing che attua specifiche prescrizioni a tutela della

riservatezza dell'identità del Segnalante e di tutti gli eventuali ulteriori soggetti coinvolti nonché del contenuto della Segnalazione e della relativa documentazione a supporto.

Sano messi a disposizione del Segnalante due diversi canali per le segnalazioni di violazioni:

- canale **ordinario**;
- canale **alternativo**, che sarà attivato solo nel caso in cui i presunti responsabili della violazione siano gli Esponenti aziendali o i membri dell'OdV/Responsabile dei Sistemi Interni di Segnalazione ed i suoi collaboratori.

Nel caso in cui il Segnalante sia corresponsabile delle violazioni, è applicato un trattamento privilegiato per quest'ultimo rispetto agli altri corresponsabili, compatibilmente con la disciplina applicabile.

L'OdV (in qualità di Responsabile dei Sistemi Interni di Segnalazione"), in via straordinaria, ovvero quando l'oggetto della Segnalazione riveste carattere di particolare gravità (es.: la segnalazione è riferita ad un processo sensibile, ci possono essere rischi, anche reputazionali, per RSI, la persona segnalata per aver commesso un presunto comportamento illegittimo appartiene all'Alta Direzione, ecc.), anche senza attendere l'esito delle indagini, riferisce direttamente e senza indugio l'informazione ricevuta, a seconda della natura della eventuale violazione o del soggetto coinvolto, agli Organi Aziendali competenti. Le informazioni oggetto di Segnalazione sono portate a conoscenza degli Organi aziendali competenti senza comunicare i dati e le informazioni riferiti al Segnalante, se questi non ne autorizza la divulgazione.

II *framework* del processo di Segnalazione è costituito dai Processi che verranno analizzati nei successivi paragrafi descrivendone nel dettaglio i sotto-processi, le attività che li compongono, gli *input* e gli *output* attesi.

6.1.1 Inserimento e invio della segnalazione

II Segnalante avvia il processo di Segnalazione attraverso la procedura informatica di Whistleblowing adottata da RSI.

II Segnalante, dopo aver scelto l'oggetto della Segnalazione, deve:

- descrivere nel dettaglio i presunti atti o fatti illeciti che ritiene opportuno segnalare dei quali è venuto a conoscenza nell'ambito delle proprie mansioni;
- fornire gli elementi che consentano l'identificazione del presunto responsabile dei fatti contestati;
- indicare, ove possibile, eventuali soggetti che possano riferire sui fatti segnalati, fornire ogni altra informazione o prova che possa costituire un utile riscontro rispetto a quanto Segnalato, avendo inoltre a sua disposizione la possibilità di allegare eventuale documentazione a supporto, a riprova di quanta affermato;
- dichiarare se ha un interesse privato collegato alla Segnalazione;
- fornire un consenso espresso, ove previsto dalla normativa, se autorizza o meno la divulgazione della propria identità. In questo caso, sono fornite al Segnalante, in forma scritta, le motivazioni alla base della eventuale necessità di disvelare la sua identità.

La tutela dell'identità è garantita anche alla persona fisica segnalata, ovvero alla persona alla quale la violazione è attribuita nella divulgazione pubblica (c.d. persona coinvolta) nonché alla relativa

documentazione a supporto. Inoltre, la riservatezza è garantita:

- al Facilitatore, sia per quanta riguarda l'identità, sia con riferimento all'attività in cui l'assistenza si concretizza;
- a persone diverse dal Segnalato, ma comunque implicate in quanto menzionate nella Segnalazione o nella divulgazione pubblica.

Con specifico riferimento alla divulgazione pubblica, la protezione della riservatezza non si applica nel caso in cui il Segnalante abbia intenzionalmente rivelato la sua identità mediante, ad esempio, piattaforme web o *social media*. Lo stesso vale nell'ipotesi in cui il Segnalante si rivolga direttamente ad un giornalista.

In qualsiasi momento il Segnalante può consultare nella procedura informatica di Whistleblowing lo stato di avanzamento della propria Segnalazione.

6.1.2 Ricezione, esame e valutazione

In questa fase, per il tramite della procedura informatica di whistleblowing adottata da RSI, al Segnalante è comunicato l'avviso di ricevimento della Segnalazione entro **sette giorni** dalla data di ricezione.

La Compliance Corporate e/o iI Response Team oppure, a seconda del caso, l'OdV (in qualità di Responsabile dei Sistemi Interni di Segnalazione) riceve la Segnalazione e svolge una valutazione **preliminare** con l'obiettivo di verificare che la stessa i) sia ammissibile secondo quanto definito nella regolamentazione aziendale di riferimento, ii) contenga elementi sufficienti per avviare un'investigazione. In particolare, è necessario accertare:

- con riferimento al punto i), che la segnalazione rientri nell'ambito di applicazione oggettivo previsto dal presente e documento;
- con riferimento al punto ii), che la Segnalazione contenga almeno i seguenti elementi: dati identificativi del Segnalante (ove applicabile) e un suo documento di identità valido, le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della Segnalazione, la descrizione del fatto, le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

Inoltre, si rappresenta che **non dovranno essere considerate** eventuali Segnalazioni ricevute che siano:

- caratterizzate da i) carenze negli elementi ritenuti essenziali per avviare l'istruttoria come, a titolo esemplificativo, incertezza dei dati identificativi del Segnalante (ove applicabile) e assenza di un documento di identità valido, eccessiva genericità e/o infondatezza dei fatti oggetto di Segnalazione, ii) manifesta insussistenza dei presupposti di legge per l'applicazione di una sanzione, iii) finalità palesemente emulativa, fatta salva l'applicazione, ove ne ricorrano i presupposti, delle sanzioni a carico del Segnalante che abbia agito con dolo o colpa grave;
- trasmesse da soggetti non appartenenti al perimetro previsto dalla normativa di riferimento (Cfr. par. 2.4.2).

Verificata l'ammissibilità della Segnalazione e la sufficienza delle informazioni contenute per avviare un'investigazione, nel rispetto dei principi di riservatezza, il Response Team oppure, a seconda del caso, l'OdV (in qualità di Responsabile dei Sistemi Interni di Segnalazione) avvia l'attività di indagine

che consiste nell'accertare i fatti tramite una ricognizione accurata e completa degli eventi segnalati e l'acquisizione in via autonoma di eventuali ulteriori dati, informazioni e/o documentazione a supporto utili per un puntuale riscontro degli elementi oggetto di Segnalazione.

Il Response Team oppure, a seconda del caso, l'OdV (in qualità di Responsabile dei Sistemi Interni di Segnalazione - canale ordinario) o la Struttura incaricata per la gestione del canale alternativo:

- stabilisce se sia in possesso delle competenze necessarie per approfondire in modo accurato e completo tutti gli elementi contenuti nella Segnalazione. In caso positivo, procede tempestivamente alla ricognizione dei fatti segnalati ed al completamento dell'indagine, entro i termini previsti dal presente documento. In relazione alla specificità della Segnalazione e per approfondire alcuni elementi, il Response Team/OdV, al fine di svolgere gli incarichi previsti dal presente Regolamento, si può avvalere del supporto di altre strutture nel rispetto dei principi di riservatezza;
- qualora non sia in possesso delle competenze necessarie per valutare in modo accurato e completo tutti gli elementi contenuti nella Segnalazione, fermo restando ii principio di riservatezza, informa tempestivamente l'Organo aziendale competente (Cfr. par. 6.1.3). Quest'ultimo provvederà ad individuare la struttura idonea a svolgere l'investigazione (cd. Funzione investigante). In questo caso, il Response Team/OdV trasmette la Segnalazione alla Funzione investigante che avvia tempestivamente le indagini, effettuando una ricognizione dei fatti segnalati e completando le attività entro i termini previsti dal presente documento. Al termine delle verifiche condotte, la Funzione investigante fornisce un riscontro scritto al Response Team/OdV, in tempo utile per il rispetto dei termini previsti dal presente documento, che i) riassuma lo svolgimento dell'indagine e le prove raccolte, ii) riporti chiaramente le conclusioni alle quali si è giunti, iii) fornisca raccomandazioni e suggerimenti sulle azioni da porre in essere per sopperire alle violazioni riscontrate ed assicurare che queste non si verifichino in futuro;
- se la Segnalazione ha un impatto anche sugli illeciti previsti dal MOG adottato ai sensi del D.Lgs. 231/2001, informa tempestivamente l'Organismo di Vigilanza per le valutazioni di competenza;
- se dalla Segnalazione dovessero emergere talune carenze dell'impianto operativo, regolamentare e procedurale, compresi i sistemi informativi, provvede ad informare le strutture competenti, senza rivelare l'identità dei soggetti coinvolti;
- provvede all'inoltro della pratica e dei relativi esiti dell'indagine agli Organi aziendali competenti che si attivano tempestivamente al fine di individuare le eventuali misure di intervento da adottare o di archiviare la Segnalazione (Cfr. Par. 6.1.3);
- provvede a fornire un riscontro al Segnalante sull'esito della Segnalazione. A titolo esemplificativo, il riscontro può consistere nella comunicazione dell'archiviazione, nell'avvio di un'inchiesta interna ed eventualmente nelle relative risultanze, nei provvedimenti adottati per affrontare la questione sollevata, nel rinvio a un'Autorità competente per ulteriori indagini.

II Response Team/OdV (ovvero il Response Team oppure, a seconda del caso, l'OdV in qualità di Responsabile dei Sistemi Interni di Segnalazione), nell'ambito della procedura informatica di whistleblowing ed in tempo utile per il rispetto dei termini previsti dal presente documento:

- riassume lo svolgimento dell'indagine e le prove raccolte;

- riporta chiaramente le conclusioni alle quali si è giunti;
- fornisce raccomandazioni e suggerimenti sulle azioni da attuare per sopperire alle violazioni riscontrate ed assicurare che queste non si verifichino in futuro.

In ogni caso, qualora il Response Team/OdV o la struttura incaricata per la gestione del canale alternativo (Presidente del Consiglio di Amministrazione o al Presidente del Collegio Sindacale), debba ricorrere ad altro personale ai fini della gestione delle segnalazioni, tale personale per tale attività dovrà essere espressamente autorizzato (artt. 4, par. l 0, 29, 32 par. 4 regolamento e art. 2-quadeterdecies del Codice) al trattamento dei dati personali e, di conseguenza, dovrà attenersi al rispetto delle istruzioni impartite, nonché di quelle più specifiche, connesse ai particolari trattamenti, eventualmente di volta in volta fornite dal Response Team/OdV. Le informazioni oggetto di Segnalazione sono portate a conoscenza delle eventuali ulteriori strutture coinvolte per le indagini senza comunicare i dati e le informazioni riferiti al Segnalante, se questi non ne autorizza la divulgazione.

Qualora sulla base delle analisi preliminari effettuate, iI Response Team/OdV valuti che la Segnalazione **non** sia ammissibile, secondo quanto previsto dal presente documento, **propone l'archiviazione** della Segnalazione all'Organo aziendale competente (Cfr. paragrafo 6.1.3) nonché di **non** procedere con ulteriori analisi, specificando, in forma scritta, la relativa motivazione. Una volta ottenuta la relativa approvazione da parte dell'Organo aziendale competente, il Response Team/OdV fornisce un'informativa al Segnalante sulla non pertinenza della Segnalazione e procede alla sua archiviazione.

Nel caso in cui alla conclusione della valutazione preliminare, il Response Team/OdV valuti l'ammissibilità della Segnalazione ma constati che la stessa **non** contenga informazioni sufficienti per avviare un'investigazione, **richiede dati, informazioni e/o documentazione a supporto integrativi** al Segnalante per il tramite della procedura informatica di whistleblowing adottata da RSI.

Inoltre, nel rispetto dei principi di tutela e riservatezza e nell'ambito della valutazione preliminare e delle fasi successive del processo, il Response Team/OdV o le eventuali ulteriori strutture coinvolte hanno la facoltà di richiedere una o più audizioni, anche in presenza, al Segnalante e/o alle eventuali ulteriori persone coinvolte e/o citate nella Segnalazione, per approfondire gli elementi ritenuti utili per una adeguata gestione della stessa. Tale facoltà è prevista anche in capo allo stesso Segnalante.

Infine, la Segnalazione inviata ad un soggetto diverso dal Response Team/OdV di RSI dalla quale emerga la chiara volontà del Segnalante di beneficiare delle tutele previste dal Decreto Legislativo 24/2023 - deve essere trasmessa a quest'ultimo con tempestività e riservatezza (entro sette giorni dal ricevimento), dando contestuale notizia della trasmissione al Segnalante.

6.1.3 Definizione delle misure di intervento

I provvedimenti decisionali sono rimessi agli Organi aziendali competenti. In coerenza con la normativa di riferimento e con quanta previsto dal Regolamento Disciplinare eventualmente adottato da RSI, sono coinvolti soggetti diversi rispetto a quelli incaricati a ricevere, esaminare e valutare la Segnalazione, come di seguito specificato:

- per il Personale della RSI (esclusi i membri dell'OdV, in qualità di Responsabile dei Sistemi Interni di Segnalazione ed i Responsabili delle Funzioni Aziendali di Controllo della Capogruppo), le decisioni competono all'Amministratore Delegato in coordinamento con la

Struttura che si occupa della gestione risorse umane;

- per i membri dell'OdV, in qualità di Responsabile dei Sistemi Interni di Segnalazione, le decisioni competono al Consiglio di Amministrazione di RSI;
- per i Responsabili delle Funzioni Aziendali di Controllo della Capogruppo, le decisioni competono al Consiglio di Amministrazione della Capogruppo;
- per l'Amministratore Delegato, i componenti del Consiglio di Amministrazione, le decisioni competono al Consiglio di Amministrazione con il parere del Collegio Sindacale di RSI (esclusi i soggetti coinvolti nella Segnalazione);
- per il Presidente e/o i componenti del Collegio Sindacale, le decisioni competono ai membri del Collegio Sindacale RSI non coinvolti nella Segnalazione.

In funzione della violazione riscontrata e dei soggetti coinvolti, sono definiti, anche avvalendosi del supporto delle Strutture/Organi aziendali competenti, i provvedimenti necessari da adottare dandone tempestiva informativa al Response Team/OdV, nel rispetto delle tutele previste nel Regolamento.

II presunto responsabile della violazione è tutelato da ripercussioni negative derivanti dalla Segnalazione nel caso in cui non emergano elementi che giustifichino l'adozione di provvedimenti nei suoi confronti.

Inoltre, a sostegno della persona segnalata e del suo diritto di difesa, tale soggetto è informato dall'Organo aziendale/Struttura competente dell'avvio di un procedimento nei suoi confronti e, in tal caso, può essere audito, anche dietro sua richiesta e/o mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

Qualora dalle verifiche condotte, secondo quanto previsto nel presente documento, si riscontri un comportamento illecito imputabile ad uno o più dipendenti, il Datore di Lavoro RSI agirà con immediatezza attraverso misure e provvedimenti sanzionatori, secondo quanto previsto dalla vigente normativa in materia di diritto del Lavoro e Contratto Collettivo Nazionale di Lavoro (CCNL) applicabile; tali misure sono applicate anche nei confronti di chi i) viola le misure a tutela del Segnalante nonché ii) attui qualsiasi forma di ritorsione nei confronti dello stesso nonché di chi effettua con dolo o colpa grave Segnalazioni che si rivelano infondate. Le misure di intervento possono prevedere, inoltre, azioni volte al rafforzamento del sistema dei controlli interni e della gestione dei rischi qualora dalle indagini siano emerse aree di debolezza.

II Segnalante ha la possibilità di consultare nel continuo lo stato e gli esiti della Segnalazione nella procedura informatica di whistleblowing a supporto. L'esito della Segnalazione è fornito compatibilmente con i ragionevoli tempi necessari per svolgere le opportune indagini. Qualora l'iter non fosse ancora concluso, andrà, tuttavia, fornito un aggiornamento entro **novanta giorni** dalla presa in carico della Segnalazione.

Si precisa che il riscontro può anche essere meramente interlocutorio, giacché possono essere comunicate le informazioni relative alle attività descritte nel precedente paragrafo che si intende intraprendere e lo stato di avanzamento dell'istruttoria. In tale ultimo caso, terminate l'istruttoria, gli esiti dovranno comunque essere tempestivamente comunicati alla persona Segnalante.

6.2 Archiviazione della documentazione

Al fine di consentire la ricostruzione delle diverse fasi del processo assicurandone la tracciabilità, tutta

la documentazione raccolta viene archiviata, a cura del Response Team/OdV, in un apposito repository, garantendo la riservatezza delta documentazione acquisita attraverso un sistema di protezione e criptatura dei dati, e deve essere accessibile solo ai Dipendenti autorizzati in virtù del proprio ruolo. L'archiviazione della documentazione avviene avvalendosi della procedura informatica di whistleblowing individuata per la gestione del processo.

Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque 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 presente decreto 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.

6.3 Registro

Il Response Team/OdV di RSI alimenta ed aggiorna un registro delle eventuali Segnalazioni ricevute, annotandone gli elementi principali delle stesse, mediante l'utilizzo della procedura informatica di whistleblowing individuata per la gestione del processo.

6.4 Relazione annuale

Con frequenza annuale, l'OdV, in qualità di Responsabile dei Sistemi Interni di segnalazione della RSI, anche sulla base delle informazioni trasmesse dalla Capogruppo, redige una relazione sul corretto funzionamento della procedura dei Sistemi Interni di segnalazione contenente, in forma anonima, le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle Segnalazioni ricevute, con evidenza della numerosità delle indagini svolte e delle tipologie dei provvedimenti adottati.

La relazione viene comunicata annualmente al Consiglio di Amministratore ed al Collegio Sindacale di RSI entro il 30 aprile, che ne prendono atto, e messa a disposizione del Personale.

7 PRESIDI DI CONTROLLO

Nel rispetto della vigente normativa devono essere assicurati i presidi per la tutela dei dati personali dei soggetti coinvolti nel processo di segnalazione:

Applicabilità del processo: resta in capo a RSI verificare nel continuo l'applicabilità di alcuni dei requisiti di cui al par. 2.4.1.

Obbligo di Riservatezza: ai sensi dell'art.12 dello Schema di Decreto 1 "le segnalazioni non possono essere utilizzate oltre quanta necessario per dare adeguato seguito alle stesse" 2 "L'identità della persona segnalante e qualsiasi altra informazione, da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rilevate, 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.

Trattamento dei dati personali: ai sensi dell'art.13 "i dati personali che manifestamente non sono utili

al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, devono essere cancellati immediatamente".

Tempistiche: la normativa prevede che entro 7 giorni dalla ricezione della segnalazione debba essere rilasciato al segnalante un avviso di ricevimento e che entro 3 mesi dalla data dell'avviso di ricevimento si debba dare riscontro alla segnalazione o, in mancanza di tale avviso, entro 3 mesi dalla scadenza del termine dei 7 giorni dalla presentazione della segnalazione.

Data retention: ai sensi dell'art 14 Conservazione della documentazione inerente alle segnalazioni, le segnalazioni, interne ed esterne e la relativa documentazione sono conservate per ii tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza.