Whistleblowing Policy

SILVATEAM

Tipo di documento	Policy	Codice documento	IA 01

Proprietario del documento	Internal Audit, Risk Management & Compliance
Revisione dei documenti	Internal Audit, Risk Management & Compliance Director Silvateam S.p.A.
Approvatore di documenti	Consiglio di Amministrazione di Silvateam S.p.A.

Versione	Data	Commenti / Modifiche
1	29/09/2021	Prima emissione
2	19/02/2024	Aggiornamento policy alla luce del D. Lgs. 24/2023

1 Premessa

Le Società del gruppo già nell'ambito del Modello ex D. Lgs. 231/01 aveva previsto il canale per consentire la comunicazione all'Organismo di Vigilanza delle violazioni del Modello e dettato le regole a tutela del segnalato e del segnalante.

A seguito dell'emanazione del Decreto Legislativo 10 marzo 2023, n, 24 che recepisce nell'ordinamento italiano la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea (cd. direttiva whistleblowing) di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato, che ledano l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, le Società hanno adottato la presente policy al fine di essere in linea con le più recenti indicazioni legislative.

Il Whistleblowing è da considerarsi come strumento fondamentale per contrastare possibili illeciti e a diffondere nei dipendenti la cultura dell'etica e della legalità all'interno delle organizzazioni, per creare un clima di trasparenza ed un senso di partecipazione e appartenenza.

2 Scopo

La presente Policy ha lo scopo di definire i principi comportamentali e modalità operative per la gestione delle segnalazioni (cd. whistleblowing), anche al fine di assicurare il perseguimento dei seguenti obiettivi di controllo:

- assicurare condizioni di legalità, correttezza e trasparenza nella conduzione delle attività aziendali;
- garantire che vengano evitate pratiche commerciali sleali, scorrette o illegali;
- prevenire le condotte corruttive e più in generale, gli illeciti.

Inoltre, si propone di disciplinare il processo di ricezione, analisi e trattamento delle segnalazioni, inviate o trasmesse, anche in forma anonima, e descrive i canali di comunicazione istituiti attraverso i quali è possibile effettuare segnalazioni ai sensi della presente Policy.

La stessa definisce le regole a cui attenersi nel processo di gestione delle segnalazioni ("Whistleblowing"), al fine di assicurare il perseguimento dei seguenti obiettivi:

- tutela del segnalante, riservatezza e protezione dalla ritorsione;
- imparzialità, trasparenza, correttezza ed eticità nel processo di ricezione e valutazione delle segnalazioni e nell'eventuale processo di investigazione delle stesse, inclusi i possibili followup (azioni correttive e / o sanzioni disciplinari);
- chiara attribuzione delle responsabilità, in coerenza con la struttura organizzativa e con le mansioni assegnate, e tenuto conto del principio di separazione delle responsabilità ("Segregation of Duties") nell'ambito di un processo;
- autorizzazione delle operazioni e tracciabilità del processo decisionale;
- assicurazione del controllo sull'effettiva applicazione del Codice Etico, delle policy e procedure di tutte le società del Gruppo Silvateam.

3 Ambito di applicazione

La Policy si applica alle società del Gruppo Silvateam ed in particolare alla società controllate e collegate che soddisfano i requisiti richiesti dal Decreto Legislativo 10 marzo 2023, n. 24 (di seguito anche collettivamente intese con il termine la "Società"). L'elenco aggiornato delle società è allegato alla presente Policy.

Con riferimento alle società italiane dotate di un Modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/01, sono escluse dalla trattazione della presente Policy gli obblighi di informativa (cd. "Flussi Informativi") verso gli Organismi di Vigilanza delle società italiane del Gruppo Silvateam, al fine di agevolarne la vigilanza sul funzionamento e l'osservanza dei Modello 231, per i quali si rimanda alla Procedura "Flussi informativi verso l'Organismo di Vigilanza".

In particolare, i destinatari (d'ora in avanti collettivamente "Destinatari") della presente policy sono quelli indicati all'interno del par. 7.1.1 e possono segnalare potenziali attività illecite che possano violare la legge, il Codice Etico o le politiche della Società. La segnalazione di possibili violazioni è incoraggiata, per consentire alla società di indagare nel merito e adottare le necessarie misure correttive. Dette misure consentono alla Società di ridurre eventuali rischi o danni per il singolo dipendente, i colleghi, la società stessa o le comunità in cui opera.

4 Termini di validità

La presente Policy, redatta tenendo conto delle disposizioni normative vigenti, assume validità dalla data di emissione (indicata in copertina): la sua validità sarà oggetto di valutazione periodica.

5 Riferimenti

- Decreto Legislativo 10 marzo 2023, n. 24
- Decreto Legislativo 231/01
- Codice Etico di Gruppo
- Modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/01

6 Principi generali di condotta

Il personale Silvateam è tenuto ad osservare, oltre alle regole esposte nel presente documento, le norme comportamentali richiamate nel Codice Etico e, ove applicabile, nel Modello 231.

In particolare, la Società, nell'ambito del processo di gestione delle segnalazioni, si ispira a criteri di trasparenza, integrità e correttezza, e si impegna a rispettare i seguenti principi generali di comportamento: comportarsi in maniera corretta, tutela del segnalante, responsabilità del segnalante e tutela del soggetto segnalato, confidenzialità, tempestività di investigazione e azione, rispetto, imparzialità e collegialità.

I segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione, penalizzazione e, in ogni caso, sarà assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente o in malafede.

Silvateam invita i segnalanti ad effettuare le segnalazioni in forma nominativa, impegnandosi a mantenere riservata l'identità del segnalante in buona fede e a tutelarlo contro ogni forma di ritorsione, discriminazione e/o di penalizzazione: il Vertice Aziendale è responsabile della prevenzione e repressione di qualsiasi forma di ritorsione nei confronti di coloro che contribuiscano all'attuazione del Codice Etico. Ugualmente, la Società potrà reagire ai sensi della normativa applicabile verso chi, consapevolmente, dovesse effettuare segnalazioni false, infondate o pretestuose.

Affinché si possa configurare una ritorsione e, di conseguenza, il soggetto possa beneficiare di protezione è necessario uno stretto collegamento tra la segnalazione, la divulgazione o la denuncia e il comportamento sfavorevole.

L'intento ritorsivo può desumersi anche dall'assenza di giustificazione o dall'infondatezza o pretestuosità delle motivazioni poste a fondamento del comportamento sfavorevole.

I segnalanti o denuncianti devono ragionevolmente credere, anche alla luce delle circostanze del caso concreto e dei dati disponibili al momento della segnalazione, divulgazione o denuncia, che le informazioni sulle violazioni segnalate, divulgate o denunciate siano veritiere. Non sono sufficienti invece semplici supposizioni o voci di corridoio così come notizie di pubblico dominio.

La tutela è estesa anche a favore di:

- Facilitatori;
- persone del medesimo contesto lavorativo;
- colleghi di lavoro;
- soggetti giuridici nei casi in cui siano enti di proprietà del segnalante, denunciante, divulgatore pubblico o enti in cui lavora o enti che operano nel medesimo contesto lavorativo.

Colui che ritiene di essere sottoposto a comportamenti discriminatori per il fatto di aver effettuato una segnalazione trasmette ad ANAC la comunicazione della misura ritorsiva attraverso la piattaforma informatica ANAC.

Eventuali segnalazioni ricevute in forma anonima saranno prese in considerazione a discrezione di Silvateam, sulla base della fondatezza, accuratezza e veridicità degli elementi forniti.

7 Processo

7.1 Whistleblower

Il whistleblower è la persona che segnala, divulga ovvero denuncia violazioni (es. comportamenti, atti od omissioni) che ledono l'integrità dell'ente privato, di cui è venuta a conoscenza nell'ambito del contesto lavorativo privato.

7.1.1 Chi può effettuare la segnalazione?

Le persone legittimate a effettuare segnalazioni e che operano nel contesto lavorativo della società sono le seguenti:

- Dipendenti;
- Lavoratori autonomi;
- Titolari di un rapporto di collaborazione che svolgono la propria attività lavorativa presso la società;
- I lavoratori o i collaboratori che svolgono la propria attività lavorativa presso la società che forniscono beni o servizi o che realizzano opere in favore di terzi;
- I liberi professionisti e i consulenti che prestano la propria attività presso la società;
- I volontari e i tirocinanti, retribuiti e non retribuiti che prestano la propria attività presso la società;
- 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, presso la società.

7.1.2 Quando si può effettuare la segnalazione?

La segnalazione, la denuncia all'autorità giudiziaria o contabile o la divulgazione pubblica di informazioni può avvenire:

- Quando il rapporto giuridico **è in corso**;
- Quando il rapporto giuridico **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 (es. pensionati).

7.1.3 Cosa si può segnalare?

Si possono segnalare comportamenti, atti od omissioni che ledono l'integrità della società e che consistono in:

- **Condotte illecite rilevanti ai sensi del D. Lgs 231 /2001** (reati presupposto a titolo esemplificativo: Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture), **o violazioni dei modelli di organizzazione e gestione**
- **Illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione Europea o nazionali** 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 (es. reati ambientali quali scarico, emissione o altro tipo di rilascio di materiali pericolosi nell'aria, nel terreno o nell'acqua oppure raccolta, trasporto, recupero o smaltimento illecito di rifiuti pericolosi);
- **Atti od omissioni che ledono gli interessi finanziari** dell'Unione come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE (es. frodi, corruzione e qualsiasi altra attività illegale connessa alle spese dell'Unione);
- **Atti od omissioni riguardanti il mercato interno** dell'Unione (es. violazioni in materia di concorrenza e di aiuti di stato)
- Atti o comportamenti che **vanificano l'oggetto o la finalità** delle disposizioni di cui agli atti dell'Unione Europea.

Le segnalazioni devono riguardare fatti di cui il segnalante abbia conoscenza diretta, avendo lo stesso fondati motivi di ritenere che le informazioni segnalate siano vere al momento della comunicazione.

Le segnalazioni devono essere effettuate tempestivamente rispetto alla conoscenza dei fatti in modo da renderne concretamente possibile la verifica.

La segnalazione, inoltre, può avere ad oggetto anche:

- Le informazioni relative alle condotte volte ad **occultare** le violazioni sopra indicate (es. occultamento o distribuzione di prove);
- Le attività illecite **non ancora compiute** ma che il whistleblower ritenga ragionevolmente possano verificarsi in presenza di elementi concreti, precisi e concordanti;
- **fondati sospetti**, che saranno oggetto di interpretazione e valutazione.

Si sottolinea che le violazioni segnalate devono incidere sull'integrità della società e non devono essere relative a contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro o inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate (es. vertenze di lavoro, discriminazioni, conflitti interpersonali tra colleghi).

7.1.4 Forme di tutela

La Società assicura la riservatezza dell'identità del segnalante, vieta ogni forma di ritorsione o discriminazione nei confronti di chiunque abbia effettuato una segnalazione e di terzi connessi al segnalante e adotta le misure volte a tutelare i diritti dei soggetti segnalati.

I soggetti a qualsiasi titolo coinvolti nella gestione delle segnalazioni sono tenuti, nei limiti previsti dalla legge, alla riservatezza in merito all'esistenza e al contenuto della segnalazione e all'attività compiuta al riguardo e garantiscono la riservatezza sull'identità del segnalante, del segnalato e degli altri soggetti coinvolti secondo quanto previsto dalla normativa vigente.

7.1.4.1 Ritorsioni

Le persone segnalanti non possono subire alcuna ritorsione e Silvateam si impegna a tutelare la persona segnalante in buona fede contro qualsiasi forma di ritorsione, discriminazione o penalizzazione per motivi collegati, direttamente o indirettamente, alla segnalazione. Costituiscono fattispecie di ritorsioni:

- Licenziamento o sospensione o misure equivalenti
- Retrocessione di grato o mancata promozione
- Mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro
- Sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa
- Note di merito negative o referenze negative
- Adozione di misure disciplinari o altre sanzioni, anche pecuniarie
- Coercizione, intimidazione, molestie o ostracismo
- Discriminazione o comunque trattamento sfavorevole
- La mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- Il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- I danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- L'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- La conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- L'annullamento di una licenza o di un permesso;
- La richiesta di sottoposizione ad accertamenti psichiatrici o medici.

In caso di ritorsioni subite nel contesto lavorativo privato, la stessa può essere comunicata all'Autorità Nazionale anticorruzione (ANAC), la quale a sua volta informa l'ispettorato nazionale del lavoro, per i provvedimenti di propria competenza.

Gli atti assunti in violazione del divieto di ritorsione sono nulli. Le persone che siano state licenziate a causa di una segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile hanno diritto a essere reintegrate nel posto di lavoro.

7.1.4.2 Protezione dalle ritorsioni

Le misure di protezione dalle ritorsioni, oltre che alla persona segnalante, sono estese, anche ai seguenti soggetti:

- Facilitatore ovvero persona fisica che assiste il segnalante nel processo di segnalazione operante all'interno del medesimo contesto lavorativo e la cui assistenza deve rimanere riservata;
- persone del medesimo contesto lavorativo della persona segnalante o di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- enti di proprietà della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché enti che operano nel medesimo contesto lavorativo delle predette persone.

Le misure di protezione si applicano quando ricorrono le seguenti condizioni:

- al momento della segnalazione la persona segnalante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate fossero vere;
- la segnalazione è stata effettuata nel rispetto della presente policy.

Le misure di protezione decadono quando è accertata la responsabilità penale della persona segnalante per i reati di diffamazione/calunnia o la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, e alla persona segnalante o denunciate è irrogata una sanzione disciplinare.

7.1.4.3 Tutela della riservatezza

Le segnalazioni non possono essere utilizzate oltre il necessario per dare adeguato seguito alle stesse. L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, senza il consenso espresso della stessa persona segnalante. Il divieto di rivelare l'identità del whistleblower è da riferirsi non solo al nominativo del segnalante ma anche a tutti gli elementi della segnalazione, dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante. Inoltre, le persone competenti a ricevere o dare seguito alle segnalazioni sono espressamente autorizzate al trattamento di tali dati ai sensi della normativa in materia di protezione dei dati personali.

L'identità della persona segnalante è tutelata anche nei procedimenti penali, contabili e disciplinari. Nell'ambito del procedimento disciplinare l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalazione sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.

Infine, è prevista la tutela anche dell'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione nel rispetto delle medesime garanzie previste in favore della persona segnalante.

7.2 Canali di segnalazione

7.2.1 Canali Interni

Al fine di consentire al segnalante di procedere con la segnalazione in modo tempestivo, la società ha messo a disposizione sul proprio sito web un apposito portale Whistleblowing raggiungibile al seguente indirizzo web: https://silvateam.openblow.it/**.**

La piattaforma Whistleblowing è un'applicazione Web-Based accessibile da qualsiasi PC e dispositivo Mobile (tablet, smartphone). La piattaforma consente la compilazione, l'invio e la ricezione delle segnalazioni oltre alla possibilità di dialogare con l'istruttore in forma anonima.

Dopo l'accesso al Portale il segnalante sarà guidato nella compilazione di un questionario formato da domande aperte e/o chiuse che gli permetteranno di fornire gli elementi caratterizzanti la segnalazione (fatti, contesto temporale, dimensioni economiche, etc.).

Il segnalante potrà o meno fornire la propria identità. In ogni caso il segnalante potrà fornire le proprie generalità in un secondo momento sempre attraverso il Portale.

Al fine di impedire l'identificazione del segnalante, l'accesso al Portale è soggetto alla politica "no-log": ciò significa che i sistemi informatici aziendali non sono in grado di identificare il punto di accesso al Portale (indirizzo IP) anche nel caso in cui l'accesso venisse effettuato da un computer connesso alla rete aziendale.

Nel momento dell'invio della segnalazione il Portale rilascerà al segnalante un codice identificativo univoco di 16 cifre (KEY CODE). Questo codice, conosciuto solamente dal segnalante, non potrà essere recuperato in alcun modo in caso di smarrimento. Il KEY CODE servirà al segnalante per accedere, sempre tramite il Portale, alla propria segnalazione al fine di:

- monitorarne lo stato di avanzamento;
- richiedere ulteriori informazioni attraverso la chat;
- fornire le proprie generalità;
- rispondere ad eventuali domande di approfondimento.

Tale KEY CODE non va assolutamente perso.

Inoltre, oltre alla piattaforma informatica delineato come canale prioritario di segnalazione in quanto ritenuto maggiormente idoneo a garantire la riservatezza del segnalante e della segnalazione, si possono effettuare le segnalazioni attraverso i seguenti canali, anche se non preferenziali:

- chiamando i seguenti numeri telefonici
  - 0174/030001 - JRS Silvateam Ingredients S.r.l.
  - 0174/030002 - Silvateam S.p.A.
  - 0174/030003 - Ledoga S.r.l.
  - 0174/030004 - Silvachimica S.r.l.

  con tecnologia Interactive Voice Response, un sistema di risposta alle chiamate tramite un Risponditore automatico. In questo caso il Risponditore automatico somministra vocalmente il questionario al Segnalante (un questionario rappresentativo di quello proposto via piattaforma), guidandolo nelle risposte vocali, dopo aver comunicato l'informativa al trattamento dei dati personali e acquisto il consenso. Infine, viene comunicato al segnalante l'inserimento della sua segnalazione in piattaforma ed il codice della segnalazione che è stato generato.
- Su richiesta dell'interessato mediante un incontro diretto con un istruttore fissato entro un termine ragionevole. L'incontro verrà verbalizzato e sottoscritto.

7.2.1.1 Contenuto della segnalazione

Il segnalante deve fornire tutti gli elementi utili a consentire di procedere alle dovute ed appropriate verifiche ed accertamenti a riscontro della fondatezza dei fatti oggetto di segnalazione.

A tal fine, la segnalazione deve preferibilmente contenere i seguenti elementi:

a) qualifica del soggetto che effettua la segnalazione;

b) descrizione dei fatti oggetto di segnalazione, con indicazione, se conosciute, delle circostanze di tempo e di luogo in cui sono stati commessi;

c) le generalità o altri elementi che consentano di identificare il soggetto/i che ha/hanno posto in essere i fatti segnalati;

d) l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;

e) eventuali persone a conoscenza dei fatti;

f) allegare eventuali documenti o file multimediali utili ai fatti;

g) ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

7.2.1.2 Gestione della segnalazione

Le segnalazioni trasmesse mediante il Portale sono ricevute dall'istruttore che gestisce le segnalazioni che provvede a dare seguito alle verifiche nel rispetto dei principi di imparzialità e riservatezza, effettuando ogni attività ritenuta opportuna. In particolare, le segnalazioni sono soggette al seguente iter istruttorio:

- dare avviso alla persona segnalante del ricevimento della segnalazione entro 7 giorni dalla data del suo ricevimento;
- mantenere le interlocuzioni con la persona segnalante e richiedere a quest'ultima, se necessario, integrazioni;
- dare diligente seguito alle segnalazioni ricevute;
- svolgere l'istruttoria necessaria a dare seguito alla segnalazione, anche mediante audizioni e acquisizione di documenti;
- dare riscontro alla persona segnalante entro 3 mesi o, se ricorrono giustificate e motivate ragioni, 6 mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei 7 giorni dal ricevimento;
- comunicare alla persona segnalante l'esito finale della segnalazione.

7.2.1.3 Caratteristiche della piattaforma

Relativamente agli aspetti legati alla Cyber Security, la piattaforma Whistleblowing è periodicamente oggetto di Application Security Assessment (ISO 27001, OWASP) dei Sistemi negli ambienti di pre-esercizio ed esercizio.

Sono riportate di seguito le principali caratteristiche di sicurezza della piattaforma:

- Data Retention Policy: Ogni segnalazione memorizzata nel Database incrementa l'attrattiva per potenziali Hacker. Le segnalazioni hanno una data di validità che può essere estesa dal Receiver, una segnalazione scaduta viene rimossa insieme a tutti i suoi dati
- Server Resiliency: Il Server è configurato in modo da rendere inoffensivi attacchi di tipo D/DOS. Richieste massive provenienti da uno stesso indirizzo IP che possano configurarsi come attacco, sono automaticamente inibite.

- Web content security: La comunicazione tra front end e back end utilizza le best practice, condivise a livello internazionale, tra cui header di sicurezza e cifratura della comunicazione con TLS 1.3.
- File Encryption: Un receiver può utilizzare la propria chiave PGP, se posseduta. Ciascun file è salvato su dicker utilizzando una chiave simmetrica casuale AES, la chiave è salvata su ramdisk
- GDPR: La Piattaforma di Whistleblowing è a norma con il regolamento generale sulla protezione dei dati (GDPR – General Data Protection Regulation, regolamento UE 2016/679)

Inoltre, il portale permette di:

- separare i dati identificativi del segnalante dal contenuto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva ricostruzione dell'identità del segnalante nei soli casi consentiti;
- gestire le segnalazioni in modo trasparente attraverso un iter procedurale definito e comunicato all'esterno con termini certi per l'avvio e la conclusione dell'istruttoria;
- mantenere, per quanto possibile, riservato il contenuto delle segnalazioni durante l'intera fase di gestione della segnalazione;
- adottare protocolli sicuri per il trasporto dei dati in rete nonché l'utilizzo di strumenti di crittografia per i contenuti delle segnalazioni e dell'eventuale documentazione allegata;
- adottare adeguate modalità di conservazione dei dati e della documentazione (fisico, logico, ibrido);
- adottare politiche di tutela della riservatezza attraverso strumenti informatici (disaccoppiamento dei dati del segnalante rispetto alle informazioni relative alla segnalazione, crittografia dei dati e dei documenti allegati);
- adottare politiche di accesso ai dati (funzionari abilitati all'accesso, amministratori del sistema informatico);
- consente al segnalante, attraverso appositi strumenti informatici, di verificare lo stato di avanzamento dell'istruttoria;
- non permette di risalire all'identità del segnalante se non nell'eventuale procedimento disciplinare a carico del segnalato e nell'ambito di un eventuale procedimento penale. In tali casi l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 c.p.p. Tale disposizione prevede l'obbligo del segreto sugli atti compiuti nelle indagini preliminari «fino a quando l'imputato non ne possa avere conoscenza e, comunque, non oltre la chiusura delle indagini preliminari» (il cui relativo avviso è previsto dall'art. 415-bis c.p.p.).:
  ciò a causa del fatto che l'identità del segnalante non può essere rivelata senza il suo consenso, a meno che la sua conoscenza non sia assolutamente indispensabile per la difesa dell'incolpato come previsto dall'art. 54-bis, co. 2, del d.lgs. 165/2001;
- attua modalità di audit degli accessi al sistema, la cui consultazione deve essere riservata esclusivamente ai soggetti che ne hanno diritto;
- avere funzionalità conformi al modello software ANAC;
- possibilità di inserimento dei dati anagrafici anche successivamente all'invio della segnalazione;
- avere HTTP Link Referrer Privacy: al fine di garantire la privacy utente, sono state prese adeguate contromisure per l'accesso a risorse esterne dall'interno della piattaforma, integrando comportamenti di oscuramento del Referrer applicativo;
- avere Header avanzati per la sicurezza: tutte le richieste vengono trattate con l'ausilio di Header avanzati per la sicurezza applicativa, come Strict-Transport-Security e X-Content-Security-Policy.

7.2.2 Grado di priorità nell'utilizzo dei canali di segnalazione ed ulteriori canali di segnalazione previsti dal D. Lgs 24/2023

I canali da utilizzare per le segnalazioni, sia in modo ordinario che prioritario, sono quelli interni messi a disposizione delle Società del Gruppo Silvateam, come descritto nel paragrafo 7.2.1 precedente. Secondo il Decreto Legislativo 24/2023, i Segnalanti hanno la possibilità di utilizzare il canale di segnalazione esterno fornito dall'Autorità Nazionale Anti Corruzione (ANAC) o di effettuare una divulgazione pubblica, ma solo in determinate circostanze specificate nei paragrafi successivi. Resta comunque la possibilità per i Segnalanti di presentare una denuncia alle autorità competenti.

In particolare, le segnalazioni possono:

- Avere ad oggetto condotte illecite o violazione del modello 231 ed essere effettuate solo attraverso il canale interno:
- Avere ad oggetto violazioni del diritto UE ed essere effettuate attraverso canale interno, esterno o divulgazione pubblica.

7.2.3 Canali Esterni

La persona segnalante, nei casi in cui ricorra una delle seguenti condizioni, può effettuare una segnalazione esterna all'Autorità nazionale anticorruzione (ANAC):

- Nell'ambito del contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna, anche se attivato, non è conforme alla legge:
- Ha già inviato una segnalazione tramite i canali di segnalazione interna ma la stessa non ha avuto seguito;
- Ha fondati motivi di ritenere che, se facesse una segnalazione interna, alla stessa, non vi sarebbe un seguito efficace oppure si ritiene che la segnalazione possa determinare il rischio di ritorsione;
- Ha fondati motivi di ritenere che la violazione potrebbe costituire un pericolo imminente o palese per il pubblico interesse.

Le segnalazioni all'ANAC possono essere trasmesse in forma scritta, compilando il modulo online appositamente predisposto sul sito dell'ANAC[1].
Nel caso in cui una segnalazione venga inviata tramite il canale di segnalazione esterna, l'ANAC procederà ad inviare alla persona segnalante un avviso di ricevimento di segnalazione entro 7 giorni dalla data di ricezione[2] e a fornire un riscontro alla segnalazione entro 3 mesi[3] dalla data di avviso di ricevimento[4] l'esito finale.

[1] L'ANAC pubblica sul proprio sito in una sezione dedicata tutte le informazioni necessarie sull'utilizzo del canale di segnalazione esterna, le modalità, i termini di scadenza per il riscontro, i tipi di riscontro, i propri contatti etc..

[2] A meno che la persona segnalante si dichiari contraria a ricevere l'avviso di ricevimento della sua segnalazione o nel caso in cui l'ANAC ritenga che l'avviso potrebbe pregiudicare la protezione della riservatezza dell'identità della persona segnalante.

[3] In mancanza di tale avviso, entro 3 mesi dalla scadenza del termine dei 7 giorni dalla presentazione della segnalazione.

[4] Nel caso in cui ricorrano giustificate e motivate ragioni, l'ANAC può fornire riscontro entro 6 mesi dalla data di avviso di ricevimento della segnalazione esterna o in mancanza di tale avviso, dalla scadenza dei sette giorni dal ricevimento.

7.2.4 Divulgazione pubblica

La persona segnalante può effettuare una divulgazione pubblica se, alla data della divulgazione, ricorre una delle seguenti condizioni:

- ha prima segnalato internamente ed esternamente o direttamente esternamente, ma non sia stata intrapresa un'azione appropriata in risposta alla segnalazione nei termini previsti dalla normativa
- ha fondati motivi di ritenere che possa esservi un pericolo imminente o palese per il pubblico interesse
- ha fondati motivi per ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto.

7.3 Istruttori delle segnalazioni

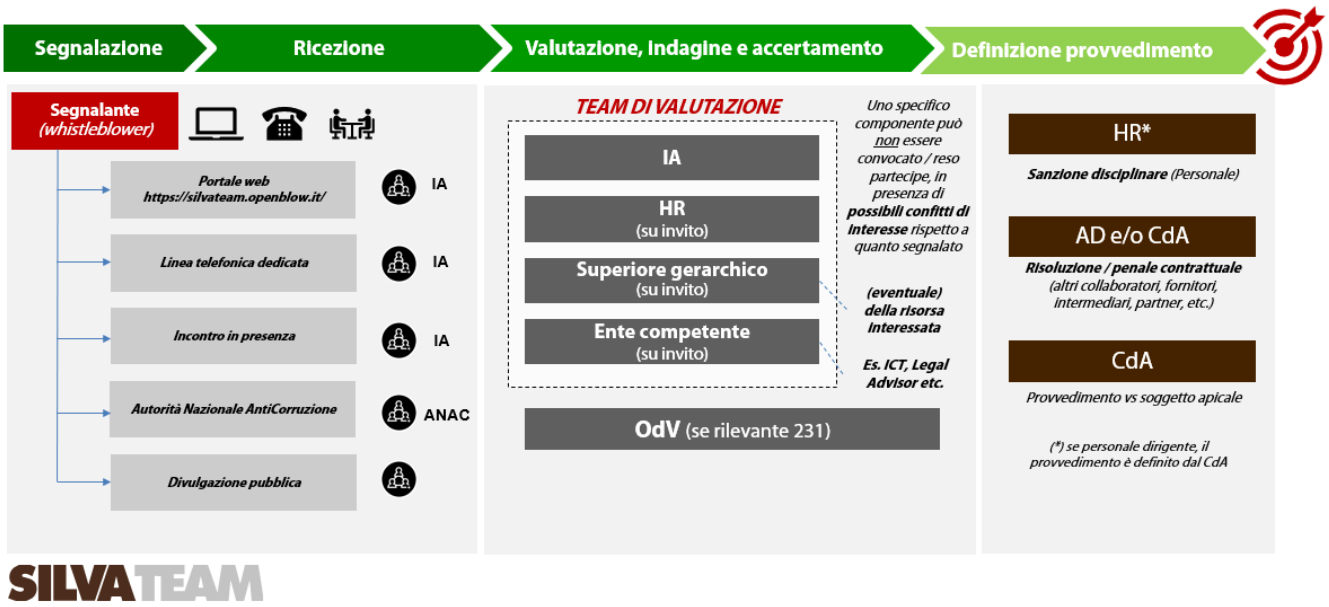
La Società ha previsto l'incarico della gestione delle segnalazioni a figure membri della funzione Internal Audit, Risk Management & Compliance, in quanto soggetti dotati di autonomia, imparzialità ed indipendenza. Tali figure in qualità di istruttori delle segnalazioni sono state adeguatamente autorizzate e nominate al trattamento dei dati personali e formate in tal senso.

Nel corso delle verifiche potranno essere coinvolti altri soggetti interni all'azienda (es. figure responsabili di struttura) per richiesta di informazioni o pareri ma rimarranno assolutamente estranei al dettaglio della segnalazione e a qualsiasi elemento che possa portare all'identificazione del soggetto segnalante. Qualora il soggetto segnalato coincida con un membro della funzione Internal Audit, Risk Management & Compliance, o nel caso in cui quest'ultimo abbia un potenziale interesse correlato alla segnalazione tale da compromettere l'imparzialità e l'indipendenza di giudizio, la segnalazione potrà essere inviata attraverso i canali predisposti e sarà indirizzata all'attenzione del Global HR Director, Ufficio Personale oppure tramite raccomandata all'attenzione del Global HR Director, Ufficio Personale, Via Torre 7, San Michele Mondovì (CN) 12080.

Il processo di Whistleblowing, relativo ad ogni singola segnalazione, si articola nelle seguenti fasi:

- segnalazione e ricezione;
- valutazione, indagine e accertamento;
- definizione del provvedimento;
- reporting periodico al CdA.

Il flusso logico di funzionamento del processo, e i relativi attori coinvolti, sono rappresentati schematicamente nella figura sottostante.



7.3.1 Segnalazione e ricezione

Le segnalazioni saranno visualizzate e gestite dal personale della Funzione Internal Audit, Risk Management & Compliance, che effettua una prima valutazione di massima circa la segnalazione, in termini di pertinenza della situazione descritta rispetto a quanto previsto dalla presente Policy, comprendendo gli elementi descrittivi che contestualizzano l'episodio o la condotta segnalata. In caso di dubbio, essi sono comunque tenuti a convocare il team di valutazione valutando eventuali conflitti di interesse.

Per le società italiane del gruppo, nel caso di segnalazioni rilevanti per uno dei reati presupposto del D. Lgs. 231/01, o comunque per il rispetto del Modello 231, il Responsabile della Funzione Internal Audit, Risk Management & Compliance informerà l'OdV per un'azione congiunta[5].

7.3.2 Valutazione, indagine e accertamento

La gestione e la verifica sulla fondatezza delle circostanze rappresentate nella segnalazione, nonché la decisione di attivare eventuali analisi di approfondimento o attività di "investigation", sono affidate, in base alla tematica:

- al Team di Valutazione. Di norma, il team è composto dai membri della Funzione Internal Audit, Risk Management e Compliance, cui si possono aggiungere, se ritenuto utile alla valutazione: (i) Global HR Director; (ii) il superiore gerarchico della risorsa (eventualmente) autrice della condotta illecita oggetto di segnalazione; (iii) il responsabile di uno specifico ente competente per la materia trattata (e.g. ICT, Legal Advisor, etc.); Il Team di Valutazione può attivare

[5] Le segnalazioni 231 saranno inviate all'OdV e saranno visualizzate dai componenti dell'Organismo di Vigilanza in carica alla data. L'OdV effettuerà una valutazione preliminare sull'oggetto della segnalazione, riservandosi la possibilità di inoltrare la segnalazione a terzi laddove lo ritenga opportuno in base all'oggetto della segnalazione ricevuta, tenendo presente la tutela della riservatezza della persona segnalante e valutando eventuali conflitti di interesse. La Funzione Internal Audit, Risk Management & Compliance e l'OdV mantengono uno stretto dialogo, e devono scambiarsi eventuali segnalazioni ricevute, laddove siano / non siano di competenza «231».

autonomamente una investigation con il coinvolgimento di Internal Auditor e/o di professionisti esterni.
- all'OdV, per le sole società italiane, che potrà avvalersi del supporto di Funzioni aziendali se lo ritiene, ovvero attivare autonomamente una investigation con il coinvolgimento di Internal Auditor e/o di professionisti esterni.

Appurata l'eventuale fondatezza della segnalazione attraverso un'istruttoria preliminare, l'ente competente svolgerà un'indagine approfondita per verificare puntualmente i contenuti della segnalazione e le possibili violazioni o comportamenti non corretti nel normale svolgimento delle attività aziendali, attivando se necessarie ulteriori specifiche attività di investigazione per l'accertamento.

Terminata la fase di indagine interna, Il Team di Valutazione si riunisce per dare una valutazione conclusiva in merito alla Segnalazione ricevuta. Le valutazioni saranno verbalizzate.

Il gestore archivia l'istruttoria, garantendo la tracciabilità delle motivazioni, nel caso in cui:

- manifesta infondatezza degli elementi di fatto;
- il contenuto della segnalazione sia generico o tale da non consentire nessun approfondimento;
- la segnalazione abbia ad oggetto fatti già trattati in procedimenti già definiti;
- vi è mancanza dei dati che costituiscono elementi essenziali della segnalazione di illeciti;
- la segnalazione non rientra tra quelle previste dal D. Lgs. n. 24/2023 per la Società.

Se procede all'archiviazione il gestore e l'OdV, qualora coinvolto, valutano se la segnalazione e la relativa documentazione (sempre garantendo la riservatezza del segnalante, dell'eventuale facilitatore e se possibile della persona coinvolta o, comunque, dei soggetti menzionati nella segnalazione) debbano essere trasmesse ad altri uffici aziendali per i profili di competenza.

La decisione deve essere comunicata al segnalante mediante la piattaforma o altro canale utilizzato per la segnalazione ed eventualmente per l'interlocuzione.

7.3.3 Definizione del provvedimento

La situazione oggetto della Segnalazione può essere riconosciuta - al termine del processo di istruttoria, indagine, valutazione e accertamento - come una

- violazione de i) Condotte illecite rilevanti ai sensi del D. Lgs 231 /2001; ii) violazioni dei modelli di organizzazione e gestione; iii) Illeciti derivanti da norme dell'Unione o nazionali; iv) Atti od omissioni che ledono gli interessi finanziari dell'Unione; v) Atti od omissioni riguardanti il mercato interno dell'Unione vi) Altro oppure
- condotta inappropriata che non configuri una vera e propria violazione come sopra descritta.

Sulla base di quanto accertato, il Team di Valutazione decide in merito alla archiviazione oppure alla opportunità di un provvedimento sanzionatorio. In quest'ultimo caso, il Team di Valutazione coinvolge il Global HR Director o l'AD/CdA (in base al rapporto che lega l'interessato a Silvateam) per le più opportune determinazioni in merito al tipo di sanzione da comminare, che saranno di entità variabile e proporzionata alla gravità del fatto, nel rispetto delle norme e dei regolamenti applicabili.

Le sanzioni nei confronti di soggetti apicali dovranno essere definite dal CdA.

7.3.4 Reporting periodico al CdA

Con cadenza semestrale o con immediatezza nel caso di urgenze, il Responsabile della Funzione Internal Audit, Risk Management e Compliance garantisce il monitoraggio e la reportistica al CdA, sempre garantendo la riservatezza del segnalante:

- delle segnalazioni pervenute
- dello stato d'avanzamento delle attività di audit / investigazione svolte sulle segnalazioni
- delle relative azioni intraprese.

8 Violazione della Policy e Responsabilità del segnalante

I dipendenti che violano la presente Policy saranno sottoposti a procedimenti disciplinari. Per gli altri Destinatari diversi dai dipendenti, la violazione della presente Policy può determinare responsabilità di natura contrattuale ed extracontrattuale.

Le segnalazioni calunniose o diffamatorie sono vietate e sanzionate secondo legge. Potranno altresì essere fonte di responsabilità in sede disciplinare, eventuali forme di abuso della presente policy, quali le segnalazioni manifestamente infondate, opportunistiche e/o effettuate al solo scopo di danneggiare il denunciato o altri soggetti, e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente policy.

9 Sanzioni

In caso di violazione delle previsioni del D. Lgs. 24/2023, l'ANAC applica al responsabile le seguenti sanzioni amministrative pecuniarie:

- Da 10.000 a 50.000 quando accerta che sono state commesse ritorsioni o quando accerta che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza;
- da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme alla normativa, nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute;
- da 500 a 2.500 euro, quando è accertata, anche con sentenza di primo grado, la responsabilità civile della persona segnalante per diffamazione o calunnia nei casi di dolo o colpa grave , salvo che la medesima sia stata già condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria.

10 Conservazione della documentazione inerente alle segnalazioni

Le segnalazioni interne ed esterne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui alla normativa europea e nazionale in materia di protezione di dati personali.

11 Definizioni

Termine	Definizione
Whistleblowing (processo di segnalazione)	Il meccanismo che consente di segnalare, purché in buona fede, «situazioni» di sospetta o presunta condotta illecita o violazione de - Normative dell'Unione Europea; - Codice Etico del Gruppo Silvateam; - ove applicabile, Modello di Organizzazione, Gestione e Controllo ex D.Lgs 231/01 (di seguito il «Modello 231»); - Policy e procedure interne; - Settori degli appalti pubblici; servizi, prodotti e mercati finanziarti e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente: radioprotezione e sicurezza alimentare; 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 sistemi informativi. da parte di un qualsiasi soggetto whistleblower così come indicato nella definizione di persona segnalante.
Situazione o violazione	Ai fini della presente Policy, si intende un fatto o una circostanza (o un insieme di elementi di fatto precisi e concordanti), cui la persona segnalante ha assistito o di cui è venuto a conoscenza, che possa costituire, se accertata come tale, una "violazione" di Leggi, Regolamenti, Codice Etico, Modello 231 ove applicabile e/o policy e procedure interne etc, secondo quanto definito sopra.
Segnalazione	Comunicazione scritta od orale di informazioni sulle violazioni effettuata ai sensi e con le modalità previste dalla presente Policy, avente ad oggetto una "Situazione" - circostanziata - che la persona segnalante ritiene meritevole di essere segnalata perché ritiene, in buona fede e sulla base di elementi di fatto precisi e concordanti, possa configurare una violazione.
Gestore del processo di segnalazione interna	Soggetto dotato di autonomia e specificatamente e adeguatamente formato alla gestione della segnalazione.
Attori del processo di segnalazione interna	Soggetti facenti parte dell'organizzazione di Silvateam, incaricati di specifiche funzioni di controllo, ovvero comunque responsabili delle funzioni preposte alla ricezione, valutazione ed indagine delle segnalazioni, secondo quanto di seguito descritto. A titolo esemplificativo e non esaustivo: - Global HR Director - Organismo di Vigilanza (di seguito anche "OdV") ai sensi del D.lgs. 231/2001, ove presente - Plant Manager - Responsabili del Servizio di Prevenzione e Protezione della Salute e Sicurezza dei lavoratori

Persona Segnalante (whistleblower)	Persona fisica che effettua la segnalazione o divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo[6].
Persona Coinvolta	Un soggetto (persona fisica o giuridica), facente parte dell'organizzazione di Silvateam o che agisca per conto di Silvateam, menzionata nella segnalazione interna o esterna o nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.
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.
Contesto lavorativo	Attività lavorative o professionali, presenti o passate attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle "situazioni".
Segnalazione interna	Comunicazione scritta o orale delle informazioni sulle "Situazioni" presentata tramite il canale di segnalazione interno.
Segnalazione esterna	Comunicazione scritta o orale delle informazioni sulle "Situazioni" presentata tramite il canale di segnalazione esterno.
Divulgazione pubblica	Rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque mezzi di diffusione in grado di raggiungere un numero elevato di persone.
Modello 231	Modello di organizzazione, gestione e controllo (ai sensi del D.Lgs. 231/2001) adottato dalle società italiane del Gruppo Silvateam.

[6] Nel dettaglio, chiunque sia collegato in senso ampio alla realtà del gruppo Silvateam, all'interno della quale si è verificata la violazione e che potrebbe temere ritorsioni in considerazione della situazione di vulnerabilità economica in cui si trova (es. Lavoratore autonomo, collaboratore esterno, liberi professionisti e consulenti, colui che svolge tirocinio (retribuito o no), volontario (retribuito o no), colui il cui rapporto di lavoro è terminato o non è ancora incominciato (ex dipendente o candidato), colui che lavora sotto la supervisione e direzione di appaltatori, sub-appaltatori, azioni e persone con funzioni di amministrazione, direzione, vigilanza o rappresentanza).