Sistemi Informativi S.r.l.
Sede Legale e Amministrativa
00148 Roma - Via Luigi Stipa, 150
Fax: 06/52206164
www.sistinf.it

Segnalazione di condotte illecite – Whistleblowing

Procedura per la gestione delle segnalazioni di condotte illecite alla luce dell'entrata in vigore del Decreto Legislativo 10 marzo 2023, n. 24

Premessa

In conformità rispetto ai requisiti di cui al Decreto Legislativo 10 marzo 2023, n. 24 entrato in vigore il 30 marzo 2023 di *"Attuazione della direttiva (UE) 2019/1937 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"* (il **"Decreto"**), questo documento ha lo scopo di indicare la modalità mediante la quale la Sistemi Informativi S.r.l. (di seguito: la **"Società"** e/o **"S.I."**) attua la procedura "Segnalazione di condotte illecite - Whistleblowing".

In tema di segnalazioni, il Decreto legislativo 8 giugno 2001, n. 231 (il **"D. Lgs. 231/2001"**) *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300"* fa, ora, rimando a tale Decreto (ai sensi dell'art. 2, comma 1, lett. a) n. 2), del Decreto).

ARTICOLO 1: Scopo e ambito

Le disposizioni del Decreto si applicano alle seguenti persone che segnalano violazioni di cui sono venute a conoscenza nell'ambito del proprio contesto lavorativo:

a) i **dipendenti delle amministrazioni pubbliche** e i dipendenti **delle autorità amministrative indipendenti di garanzia, vigilanza o regolazione**;
b) i **dipendenti degli enti pubblici economici**, degli **enti di diritto privato sottoposti a controllo pubblico**, **delle società in house, degli organismi di diritto pubblico o dei concessionari di pubblico servizio**;
c) i **lavoratori subordinati di soggetti del settore privato**;
d) i **lavoratori autonomi**, nonché i titolari di un **rapporto di collaborazione**, che svolgono la propria attività lavorativa presso soggetti del **settore pubblico** o **privato**;
e) i **lavoratori o i collaboratori**, che svolgono la propria attività lavorativa presso soggetti del **settore pubblico** o **privato** che **forniscono beni o servizi o che realizzano opere in favore di terzi**;
f) i **liberi professionisti** e i **consulenti** che prestano la propria attività presso soggetti del **settore pubblico** o **privato**;
g) i **volontari e i tirocinanti**, retribuiti e non retribuiti, che prestano la propria attività presso soggetti del **settore pubblico** o **privato**;
h) gli **azionisti** e le **persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza**, anche di mero fatto, presso soggetti del **settore pubblico** o del **settore privato**.

Inoltre, la tutela prevista dal Decreto - per i segnalanti - si applica anche:

a) quando il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante le fasi precontrattuali;

b) durante il periodo di prova;
c) successivamente allo scioglimento del rapporto giuridico, se le informazioni sono state acquisite nel corso del rapporto stesso.

Tali soggetti Interessati, accedono alle modalità di esercizio delle proprie facoltà attraverso l'informativa presente sulla Intranet e/o sul sito Internet come indicato all'articolo 3 del presente documento.

Il presente documento ha lo scopo di illustrare la procedura predisposta dalla Sistemi Informativi per consentire - ai soggetti sopra citati - di segnalare fatti o condotte di cui siano venuti a conoscenza, che possano costituire violazioni ai sensi del Decreto.

Ai sensi del Decreto, la segnalazione può essere agevolata da un "facilitatore", ovvero da un soggetto che opera all'interno del medesimo contesto lavorativo e assiste il segnalante nel processo di segnalazione.

ARTICOLO 2: Oggetto, elementi e caratteristiche delle segnalazioni

Ai sensi di quanto previsto dal Decreto, tramite il canale di comunicazione interna messo a disposizione dalla Società, è possibile effettuare segnalazioni relative a:

i. violazioni di fonti normative nazionali e dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui si sia venuti a conoscenza in un contesto lavorativo pubblico o privato;
ii. violazioni di fonti normative nazionali di attuazione degli atti dell'Unione Europea elencati nell'allegato alla Direttiva 2019/1937, in materia di: 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;
iii. atti od omissioni che ledono gli interessi finanziari dell'Unione Europea;
iv. atti od omissioni riguardanti il mercato interno (comprese le violazioni in materia di concorrenza e di aiuti di Stato e quelle in materia di imposta sulle società);
v. atti o comportamenti che, pur non integrando un illecito, vanificano l'oggetto e le finalità delle leggi e dei regolamenti nazionali e dell'Unione Europea (per un'elencazione dettagliata degli atti si fa rinvio sempre all'elenco contenuto nell'allegato al decreto legislativo n. 24/2023), nonché di quelli a tutela degli interessi finanziari dell'Unione Europea e che regolano il mercato interno;
vi. illeciti amministrativi, contabili, civili o penali che non rientrano in quelli contemplati dai punti precedenti;
vii. condotte illecite ai sensi del D. Lgs. n. 231/2001 e violazioni dei modelli di organizzazione, gestione e controllo adottati ai sensi dello stesso.

In linea con quanto previsto dal Decreto, la presente procedura non si applica alle segnalazioni aventi ad oggetto:

a) contestazioni, rivendicazioni o richieste legate a 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;

b) le violazioni di norme già disciplinate in via obbligatoria dagli atti dell'Unione Europea o nazionali indicati all'interno dell'allegato II del Decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione Europea indicati nella parte II dell'allegato dalla Direttiva (UE) 2019/1937;
c) le violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o sicurezza nazionale.

Per il tipo di segnalazione di cui al punto a) – come indicato nell'informativa – in azienda è previsto un apposito canale di comunicazione presente nella Intranet aziendale denominato *"Open Door"*.

Le segnalazioni possono essere presentate sia in forma scritta che in forma orale utilizzando il canale interno indicato all'articolo 3 della presente procedura, sempre nel rispetto della massima riservatezza e possono riguardare sia le violazioni commesse, sia quelle non ancora commesse che il segnalante, ragionevolmente, ritiene che potrebbero esserlo sulla base di elementi concreti.

Oltre alle informazioni sopra riportate, il segnalante può allegare alla segnalazione documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché indicare altri soggetti potenzialmente a conoscenza degli stessi.

Le misure di riservatezza applicate nella gestione dell'intero processo per il Segnalante sono, di conseguenza, estese a tutti i soggetti eventualmente coinvolti

Le segnalazioni devono essere il più possibile dettagliate e circostanziate, al fine di consentire ai soggetti preposti di valutare i fatti e di adottare le azioni necessarie.

In particolare, è necessario che la segnalazione contenga e fornisca chiare informazioni su:

- le circostanze di tempo e di luogo in cui si è verificato il fatto o i fatti oggetto di segnalazione;
- la descrizione dei fatti;
- le generalità o altri elementi che consentano di identificare il soggetto o i soggetti a cui attribuire i fatti segnalati;
- altri soggetti a conoscenza dei medesimi fatti;
- ogni altra informazione che possa fornire un utile riscontro ai fini della ricostruzione e successiva verifica dei fatti riportati, inclusi eventuali documenti da allegare alla segnalazione che possano fornire elementi di fondatezza dei fatti segnalati.

Anche le segnalazioni anonime saranno considerate e gestite dalla Società, a condizione che sia possibile identificare rilevanza e fondatezza delle allegazioni e che gli elementi di fatto che attengono alla segnalazione siano sufficientemente dettagliati. In questo caso, la gestione della segnalazione sarà soggetta a precauzioni idonee a preservare gli interessi di tutti i soggetti coinvolti.

La gestione della segnalazione sarà, comunque, soggetta a precauzioni idonee a preservare gli interessi di tutti i soggetti coinvolti.

ARTICOLO 3: Il canale di segnalazione interna

La Sistemi Informativi incoraggia l'utilizzo del canale di segnalazione interna, sia in **forma scritta** che in **forma orale**, come indicato sulla Intranet aziendale e sul sito Internet della Società.

Ogni segnalazione rimarrà strettamente confidenziale e conosciuta unicamente dal *Gestore delle segnalazioni*[1] e dalle persone, che compongono di volta in volta il team, che dovranno necessariamente essere coinvolte per investigare sulla segnalazione stessa.

3.1 Segnalazione scritta

La segnalazione potrà essere inoltrata tramite posta elettronica all'indirizzo e-mail Confidentially-Speaking@sistinf.it compilando l'apposito Form, che viene reso disponibile, in ogni sua parte al fine di garantire la corretta gestione della stessa. Il Form dovrà essere crittografato e sarà necessario inviare due e-mail separate: la prima contenente il Form crittografato e la seconda solo con la password (senza alcun allegato).

Istruzioni di protezione per Windows:

a) aprire il documento di Office che si desidera proteggere;
b) fare clic sul menu **File**, selezionare la scheda **Informazioni**, quindi selezionare il pulsante **Proteggi documento;**
c) fare clic su **Crittografa con password;**
d) immettere la password due volte, quindi fare clic su **OK.**
e) Attenzione! La password deve essere inviata con un'altra e-mail.

Istruzioni di protezione per Mac:

a) aprire il documento di Office che si desidera proteggere;
b) aprire il menu **Revisione;**
c) fare clic su **Proteggi documento;**
d) immettere la *passphrase* desiderata due volte, nel campo **Password**, quindi fare clic su **OK.**
e) Attenzione! La password deve essere inviata con un'altra e-mail.

Il Form può essere consegnato anche in modalità posta ordinaria oppure recapitato a mano al seguente indirizzo:

Sistemi Informativi S.r.l.
Via Luigi Stipa, 150
00148 Roma (RM)
alla cortese attenzione: *Gestore delle segnalazioni del Programma Confidentially Speaking – Whistleblowing*

La segnalazione deve essere inserita in due buste chiuse, includendo:

a) nella prima, i dati identificativi del segnalante, unitamente a un documento di identità;
b) nella seconda, l'oggetto della segnalazione.

Entrambe le buste dovranno, poi, essere inserite in una terza busta riportando, all'esterno, la dicitura *"Riservata al Gestore delle segnalazioni"*.

[1] Persona specificamente formata per questo tipo di attività e appositamente identificata sulla base di quanto previsto all'art. 4, comma 2 (Canali di segnalazione interna) e all'art. 5 (Gestione del canale di segnalazione interna) del D. Lgs. 24/2023.

3.2 Segnalazione orale

È possibile chiedere al Gestore delle segnalazioni – sempre tramite posta elettronica all'indirizzo e-mail Confidentially-Speaking@sistinf.it, oppure via telefono al numero indicato – di essere sentito personalmente per l'effettuazione della segnalazione orale.

A tal fine, è messo a disposizione il seguente numero telefonico: ***+39 347 7954718***

Previo consenso della persona segnalante, le segnalazioni orali possono essere documentate e trascritte.

3.3 Modalità di gestione della segnalazione

Una volta inviata la segnalazione, secondo una delle modalità sopra descritte, il Gestore delle segnalazioni svolge le seguenti attività:

a) rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;

b) mantiene le interlocuzioni con la persona segnalante e – laddove necessario – può richiedere integrazioni;

c) dà diligente seguito alle segnalazioni ricevute;

d) fornisce riscontro alla segnalazione entro 3 mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro 3 mesi dalla scadenza del termine dei 7 giorni dalla presentazione della segnalazione.

Nel caso il segnalante optasse per la segnalazione in forma anonima, non essendo nota la sua identità, non sarà possibile al Gestore delle segnalazioni richiedere maggiori dettagli e/o chiarimenti, né fornire un *feedback* in merito alla segnalazione stessa. L'impossibilità di contattare il segnalante per eventuali ulteriori chiarimenti potrebbe avere un impatto sulla prosecuzione delle indagini. In tal caso, l'indagine si baserà esclusivamente sulle informazioni ricevute: è, perciò, importante che il segnalante fornisca informazioni sufficienti per garantire la possibilità di dare seguito alle necessarie verifiche interne.

Considerando la materia oggetto delle segnalazioni, l'identità del segnalante rimarrà strettamente confidenziale e conosciuta unicamente dal Gestore delle segnalazioni e dalle direzioni che dovranno necessariamente essere coinvolte - ai fini legali - per investigare sulla segnalazione stessa.

Al fine di garantire l'integrità del programma, l'identità del segnalante (o informazioni da cui possa evincersi) non verrà fornita dal Gestore delle segnalazioni a persone diverse da quelle competenti e autorizzate dalla legge senza sua specifica autorizzazione.

Le attività connesse alla gestione delle segnalazioni in ambito Whistleblowing, inclusa la comunicazione tra autorità competenti, possono implicare il trattamento di dati personali di vari soggetti interessati: il segnalante, la persona coinvolta e i terzi menzionati nella segnalazione, ad esempio testimoni o colleghi. Anzitutto, in applicazione del principio di minimizzazione, i dati personali che manifestatamente non sono utili al trattamento di una specifica segnalazione non devono essere indicati e se ricevuti o accidentalmente raccolti, andranno immediatamente cancellati.

Per ulteriori dettagli relativi al trattamento dei dati personali in occasione dell'utilizzo del canale, si rimanda all'informativa Privacy Generale ai Dipendenti che viene resa disponibile.

ARTICOLO 4: L'indagine conseguente ad una sospetta violazione

4.1 Valutazione preliminare e gestione della segnalazione

Tutte le segnalazioni, una volta ricevute dal Gestore, sono soggette a una valutazione preliminare condotta da un team, composto di volta in volta, a seconda dell'argomento oggetto della segnalazione (evitando un eventuale conflitto di interessi, secondo il criterio dell'*one level up*).

Qualora dovesse pervenire, al Gestore delle segnalazioni, una segnalazione di condotta illecita rilevante ai sensi del D. Lgs. 231/2001 o avente ad oggetto violazioni del Modello 231, lo stesso ne informerà tempestivamente l'Organismo di Vigilanza *ex* D. Lgs. 231/2001.

Laddove vi sia il dubbio che la segnalazione effettivamente sia riferibile al D. Lgs. 231/2001, il Gestore delle segnalazioni potrà consultare la Direzione Legale IBM per richiederne conferma o, se necessario, uno studio legale esterno.

La segnalazione interna, presentata tramite un canale diverso da quello indicato all'articolo 3 della presente procedura, deve essere trasmessa al Gestore delle segnalazioni senza indebito ritardo e, comunque, in maniera tale che il Gestore delle segnalazioni possa dare riscontro entro 7 giorni, come previsto dal D. Lgs. 24/2023.

4.2 Indagine

Le indagini sono condotte dal team all'uopo costituito. I componenti del team sono assoggettati a speciali obblighi di riservatezza in relazione all'indagine (come esposto al successivo articolo 5). Solo investigatori che non si trovino in conflitto di interesse, rispetto ad una determinata indagine, possono far parte del team assegnato all'indagine stessa.

Gli investigatori assegnati all'analisi di una determinata segnalazione conducono interviste di soggetti che possano avere informazioni rilevanti, raccolgono ed esaminano documenti rilevanti ai fini dell'indagine per stabilire i fatti ad essa relativi. I partecipanti all'indagine possono comunicare con gli investigatori durante l'indagine con qualsiasi mezzo utile, incluso via e-mail o verbalmente.

Il processo di indagine è sempre soggetto alla supervisione del Gestore delle segnalazioni. Nel caso di segnalazioni aventi ad oggetto condotte illecite rilevanti ai sensi del D. Lgs. 231/2001 o violazioni del Modello 231, l'Organismo di Vigilanza *ex* D. Lgs. 231/2001 sarà tenuto costantemente informato sulle modalità e sugli esiti dell'indagine nonché sulle eventuali azioni intraprese a seguito della segnalazione, in conformità alla presente procedura.

Le evidenze raccolte vengono analizzate per comprendere la situazione, per stabilire se si sia effettivamente verificata una violazione rilevante ai sensi delle norme richiamate da questa procedura e ai sensi dell'articolo 2, nonché per identificare misure idonee a rimediare alla situazione che si sia determinata e/o ad evitare che una simile situazione possa ripetersi in futuro.

4.3 Conclusione dell'indagine ed esiti

A seguito dell'esame delle evidenze raccolte nell'indagine, si procede ad una condivisione confidenziale dei dati raccolti e delle risultanze ottenute da parte del Gestore delle segnalazioni.

Su proposta del Gestore delle segnalazioni, previa condivisione con l'Organismo di Vigilanza *ex* D. Lgs. 231/2001 per le segnalazioni aventi rilevanza 231, il Direttore Risorse Umane (sentito il Direttore della Funzione a cui appartiene la persona coinvolta) decide le misure successive. Se necessario, vengono

assunti provvedimenti disciplinari, per il caso specifico, che possono arrivare anche al licenziamento in casi di particolare gravità. In caso di conflitto di interessi, tra le funzioni, viene coinvolto direttamente il legale rappresentante.

Qualora la segnalazione abbia ad oggetto reati finanziari, reati tributari o illeciti contabili in genere, le risultanze e gli esiti delle indagini verranno condivise anche con il Collegio Sindacale della Società.

Nel caso in cui la segnalazione si riveli infondata e tale infondatezza sia riconducibile a dolo o colpa grave, la Società disporrà sanzioni disciplinari anche nei confronti dell'autore della segnalazione. Sono comunque vietate, in ogni caso, misure ritorsive o discriminatorie di qualsiasi tipo nei confronti del segnalante.

Non tutte le violazioni, pur se accertate, determinano sanzioni disciplinari.

ARTICOLO 5: Riservatezza

La Società garantisce la tutela della riservatezza dell'identità del segnalante, dell'identità della persona o delle persone fisiche segnalate o menzionate nella segnalazione.

L'identità della persona segnalante e qualsiasi altra informazione da cui questa possa evincersi, direttamente o indirettamente, non possono essere rivelate senza il consenso espresso dello stesso segnalante, a soggetti diversi da quelli competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzati 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.

Inoltre, la Società si impegna ad applicare gli specifici obblighi di riservatezza previsti dal Decreto in caso di procedimenti penali e procedimenti disciplinari.

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e, comunque, non oltre cinque anni (salvo, sempre, cause legittime di interruzione del decorso stesso o applicazione di diversi specifici obblighi di legge per la conservazione) a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

ARTICOLO 6: Condizioni per la protezione del segnalante

Le misure di tutela previste dal Decreto (tra cui a titolo esemplificativo la tutela della riservatezza e la tutela da qualsivoglia misura ritorsiva) si applicano al segnalante a condizione che:

a) al momento della segnalazione, l'autore della segnalazione avesse fondato motivo di ritenere che le informazioni sulle violazioni segnalate o denunciate fossero vere e rientrassero nell'ambito delle violazioni di cui all'articolo 2 della presente procedura;
b) la segnalazione è stata effettuata in conformità a quanto previsto dalla presente procedura e dal Decreto.

Le misure di tutela trovano applicazione anche in caso di segnalazione anonima, se la persona segnalante è stata successivamente identificata e ha subito ritorsioni.

ARTICOLO 7: Buona fede e divieto di ritorsioni

Chiunque sia contattato da un investigatore nell'ambito di una indagine è tenuto a collaborare in buona fede.

Un uso - in buona fede - del canale di segnalazione non determina alcuna misura disciplinare nei confronti del segnalante, anche ove l'indagine non accertasse alcuna violazione.

È vietato qualsiasi atto di ritorsione o discriminazione anche solo tentato o minacciato nei confronti di chiunque effettui - in buona fede - una segnalazione di condotte illecite in conformità alla presente procedura o al Decreto nonché nel caso in cui collabori alla stessa o ad una indagine su tali condotte.

L'autore di un atto di discriminazione o ritorsione è soggetto a serie sanzioni.

Gli atti assunti in violazione del divieto di ritorsione sono nulli.

L'uso improprio o illecito di una segnalazione o qualsiasi interferenza con una investigazione possono esporre l'autore di simili comportamenti a sanzioni o misure delle autorità.

ARTICOLO 8: Segnalazione esterna

La Sistemi Informativi incoraggia l'utilizzo del canale di segnalazione interna di cui all'articolo 3 della presente procedura. Si segnala che il Decreto prevede un canale di segnalazione esterno, gestito dall'ANAC (link per accedere al canale di segnalazione esterno e per avere maggiori informazioni).

Il ricorso a tale canale può avvenire solo se:

- il canale interno di segnalazione Whistleblowing non risulta attivo o, anche se attivo, non è conforme ai requisiti di cui all'art. 4 del Decreto;
- la persona segnalante ha già effettuato una segnalazione tramite il canale indicato all'articolo 3 e non ha avuto seguito;
- la persona segnalante ha fondati motivi di ritenere che se effettuasse una segnalazione interna, tramite il canale di cui all'articolo 3 della presente procedura, alla stessa non verrebbe dato seguito ovvero la segnalazione possa determinare il rischio di ritorsione;
- la persona segnalante ha fondato motivo di ritenere che la violazione da segnalare possa costituire un pericolo imminente o palese per l'interesse pubblico.

Si precisa che le segnalazioni riguardanti condotte rilevanti ai sensi del D. Lgs. 231/2001 e violazioni del Modello 231 non potranno essere segnalate tramite il canale esterno istituito presso l'ANAC.

ARTICOLO 9: Informativa ai potenziali utenti del canale di segnalazione

Una chiara e completa informativa viene fornita a tutti i potenziali utilizzatori del canale di segnalazione.

Le informazioni sulla procedura di segnalazione sono rese accessibili a tutti e disponibili sulla Intranet aziendale nonché sul sito Internet della Società.

****

Procedura aggiornata ed approvata dal CEO della Sistemi Informativi nel mese di dicembre 2023.