

PROCEDURA

Whistleblowing

Soggetto emittente	Consiglio di Amministrazione di Intellera Consulting Spa
Soggetto preposto al monitoraggio	Organismo di Vigilanza e Funzione Anticorruzione (RAC)
Versione	3.0
Stato	Emessa
Prima Emissione	29/04/2022
Aggiornamenti	V 2.0 del 15/05/2023 V 3.0 del 13/05/2024
Destinatari	Professionisti, Personale amministrativo e di supporto, stagisti e collaboratori, portatori di interesse a vario titolo
Codice del documento	RM_Whistleblowing_Proc_14

1. DEFINIZIONI

Con il termine Whistleblowing (di seguito anche “segnalazione”) si intende qualsiasi segnalazione, proveniente da chiunque, riguardante comportamenti (di qualsivoglia natura, anche meramente omissivi) riferibili al personale di Intellera Consulting Spa (nel seguito anche solo “Intellera” o “Società”) e/o a Terzi non conformi/in violazione a leggi e regolamenti, al Codice Etico ed al Modello Organizzativo 231, nonché al sistema di regole e procedure vigenti della Società.

Il Decreto Legislativo n. 24 del 2023 (nel seguito anche “Decreto Whistleblowing” o “Decreto”), in attuazione della Direttiva UE 2019/1937, rivisita la disciplina nazionale previgente in materia di segnalazioni di reati e irregolarità e prevede un nuovo regime di protezione rafforzato per i soggetti che segnalano condotte improprie di cui siano venuti a conoscenza nell’ambito del contesto lavorativo (d’ora in poi anche il “Segnalante” o i “Segnalanti”).

Il Decreto ha l’obiettivo di incentivare le segnalazioni di violazioni di disposizioni normative nazionali o dell’Unione Europea che ledono l’interesse pubblico o l’integrità dell’amministrazione pubblica o dell’ente privato (d’ora in poi anche la “Segnalazione” o le “Segnalazioni”) innalzando, al contempo, il livello di protezione di cui beneficiano i Segnalanti, ove ne sussistano i presupposti.

Il rafforzamento della tutela per la segnalazione di tali violazioni opera essenzialmente imponendo agli enti specifiche regole relative alle procedure di segnalazione e stabilendo il regime applicabile in caso di ritorsioni.

Al di là delle disposizioni normative, Intellera, in linea con i propri valori, incoraggia la segnalazione di condotte e comportamenti impropri e contrari alle norme di legge, tutelando la posizione dei Segnalanti in buona fede e assicurando loro la massima tutela.

Tutto il personale può suggerire modifiche/miglioramenti alla procedura scrivendo alla casella di posta procedure@intelleraconsulting.com.

2. SCOPO DEL DOCUMENTO

Il whistleblowing è un atto con cui il soggetto interno all’ente contribuisce a far emergere e a prevenire rischi e situazioni pregiudizievoli per l’ente stesso. Lo scopo principale del whistleblowing è, quindi, quello di risolvere (o, se è possibile, di prevenire) i problemi creati da un’irregolarità di gestione, permettendo di affrontare le criticità rapidamente e con la necessaria riservatezza.

La presente procedura, pertanto, è stata predisposta per regolamentare la gestione della segnalazione di irregolarità, a partire dal momento in cui il segnalante si determini all’inoltro sino ai successivi sviluppi.

La presente procedura è finalizzata anche a dare attuazione:

- alla 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”) che, a tutela dei dipendenti che segnalano presunti illeciti, ha previsto la disciplina del c.d. whistleblowing nel settore privato, modificando il D.lgs. n. 231/2001 sulla responsabilità “amministrativa” degli enti;

- al D.lgs. 24/2023 e ss.mm.ii., attuativo della direttiva (UE) 2019/1937 che abroga alcune disposizioni del d.lgs. n. 231/2001 e della legge n. 179/2017, e alle successive Linee Guida ANAC di luglio 2023.

3. DESTINATARI

La presente procedura si applica a tutto il personale Intellera (inclusi lavoratori autonomi, collaboratori e stagisti) e a ogni altro portatore di interesse di Intellera.

Possono inoltre effettuare le segnalazioni:

- i candidati (se le informazioni sulle violazioni sono state acquisite durante il processo di selezione);
- gli ex dipendenti (se le informazioni sulle violazioni sono state acquisite nel corso del rapporto di lavoro);
- i tirocinanti e i volontari, anche non retribuiti;
- i fornitori di beni e servizi e i consulenti;
- i soci e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza (anche di fatto).

4. PRINCIPI

Il whistleblowing è uno strumento di derivazione anglosassone attraverso il quale i dipendenti di una organizzazione, pubblica o privata, segnalano a specifici individui o organismi (compresi organi di polizia e autorità pubbliche) una possibile frode, un reato, un illecito o qualunque condotta irregolare, commessa da altri soggetti appartenenti all'organizzazione. I dipendenti, intesi in senso ampio, normalmente sono le prime persone che vengono a conoscenza di eventuali situazioni di rischio e, pertanto, sono anche le prime persone in grado di segnalarle tempestivamente all'organizzazione, prima che possano realizzarsi danni.

Lo scopo del whistleblowing è quello di permettere alle organizzazioni di affrontare il problema segnalato il prima possibile, rendendo note situazioni di rischio o di danno e contribuendo alla prevenzione e al contrasto di eventuali illeciti.

La gestione virtuosa del whistleblowing contribuisce non solo ad individuare e contrastare possibili illeciti e a diffondere la cultura dell'etica e della legalità all'interno delle organizzazioni, ma anche a creare un clima di trasparenza ed un senso di partecipazione e appartenenza, generato dal superamento del timore dei dipendenti di subire ritorsioni da parte degli organi sociali o dei colleghi, o dal rischio di vedere inascoltata la propria segnalazione.

Il D.Lgs. n. 24/2023, in particolare, prevede:

- che gli enti del settore privato (ma anche quelli del settore pubblico) attivino propri canali di segnalazione, 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. Anche il Modello di Organizzazione e Gestione ex D.Lgs. 231/2001 (nel seguito anche MOG 231/2001 o MOG 231 o Modello 231) di Intellera prevede canali di segnalazione interna di cui al D.Lgs. 24/2023;

- di affidare a un soggetto appositamente formato e autonomo la gestione del canale di segnalazione: nel caso di Intellera si è scelto di affidare la gestione del canale di segnalazione interna all'Organismo di Vigilanza, ai fini della presente procedura denominato anche "Comitato di gestione delle segnalazioni whistleblowing" o anche solo "Comitato Whistleblowing". L'Organismo di Vigilanza (nel seguito anche "OdV") è dunque l'organo preposto alla raccolta delle segnalazioni, ferme le responsabilità e le prerogative del Collegio Sindacale sulle segnalazioni allo stesso indirizzate, ivi incluse le denunce ex art. 2408 Codice Civile. Eventuali segnalazioni interne presentate ad un soggetto diverso sono trasmesse, entro sette giorni dal ricevimento, al soggetto competente, dando contestuale notizia della trasmissione alla persona segnalante. I componenti del Comitato Whistleblowing sono soggetti specificamente autorizzati al trattamento dei dati personali e appositamente istruiti per le attività connesse alla gestione delle segnalazioni. L'OdV, nel ruolo di Comitato Whistleblowing, gestirà le segnalazioni in conformità allo standard ISO 37008¹;
- il divieto di atti ritorsivi o discriminatori², diretti e indiretti, nei confronti del Segnalante per motivi collegati direttamente o indirettamente alla segnalazione;
- sanzioni disciplinari per chi violi le misure di tutela del segnalante e per chi effettui con dolo o colpa grave segnalazioni che si rivelino infondate.

La Procedura si applica anche alle segnalazioni anonime³, come previsto dalla ISO 37001, ove queste siano adeguatamente circostanziate, ove cioè siano in grado di far emergere fatti e situazioni relazionandoli a contesti determinati.

¹ Lo standard ISO 37008 "*Internal investigations of Organizations - Guidance*" contiene le linee guida per lo svolgimento di *internal investigations* all'interno di qualsiasi organizzazione e, dunque, le regole base applicabili a qualsiasi entità giuridica, di qualunque tipo, dimensione, e settore di riferimento per mantenere un efficace sistema di compliance e di controlli interni, oltre che per supportare coloro che devono gestire segnali d'allarme all'interno della società.

² Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.

³ Il D.Lgs. 25 maggio 2017 n. 90, emanato per dare attuazione alla Direttiva 2015/849 del Parlamento Europeo e del Consiglio del 20 maggio 2015, ha introdotto importanti novità all'interno del D.Lgs. 231/2007 contenente la normativa vigente in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Tra tali novità, il riformato art. 48 del D.Lgs. 231/2007 e s.m.i. prevede l'introduzione di un sistema di segnalazione di violazioni c.d. "whistleblowing" affine a quello introdotto dall'art. 6 nell'ambito del D.Lgs. 231/2001: in tal senso, il citato art. 48 dispone che ogni soggetto obbligato dalla normativa antiriciclaggio debba adottare "*procedure [...] per la segnalazione di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo*", che siano in grado di garantire:

- a) la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto delle segnalazioni;
- b) la tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
- c) lo sviluppo di uno specifico canale di segnalazione, anonimo e indipendente, proporzionato alla natura e alle dimensioni del soggetto obbligato.

È richiesto quindi che detto sistema di procedure (per quanto simile a quello sopra delineato per la segnalazione di violazioni ex D.Lgs. 231/2001) debba prevedere a tutela del segnalante lo sviluppo di un canale di segnalazione anonimo e indipendente.

A tal fine, e in conformità alle Linee Guida ANAC luglio 2023, Intellera si è dotata di uno strumento informatico dedicato, la Piattaforma Whistleblowing (nel seguito anche solo “Piattaforma”), che consente la possibilità di acquisizione di segnalazioni orali e/o anonime effettuate attraverso sistemi di messaggistica vocale e la comunicazione diretta con il Comitato whistleblowing.

Tale Canale garantisce la riservatezza delle Segnalazioni effettuate e della relativa documentazione (relativamente a identità del Segnalante, persone coinvolte o persone comunque menzionate nella Segnalazione, nonché al contenuto della stessa), anche tramite il ricorso a strumenti di crittografia della Piattaforma adottata.

5. CONTENUTO DELLA PROCEDURA

OGGETTO DELLA SEGNALAZIONE

Le segnalazioni che rientrano nel perimetro del whistleblowing riguardano qualsiasi comportamento illegittimo che arrechi o che possa arrecare danno o pregiudizio a Intellera e/o ai suoi dipendenti.

Per Comportamento Illegittimo si intende qualsiasi azione o omissione, avvenuta nello svolgimento dell’attività lavorativa o che abbia un impatto sulla stessa che:

- sia illecita, scorretta o immorale;
- violi le disposizioni normative e regolamentari (es. D. Lgs. 231/2001);
- non sia conforme alle normative interne (es. Codice Etico).

A titolo meramente esemplificativo, si elencano alcune fattispecie di irregolarità che potrebbero essere oggetto di segnalazione:

- percepire o dare indebitamente denaro o altre utilità a consulenti fornitori;
- compiere attività disoneste o ingannevoli;
- falsificare dati e/o informazioni relative alla clientela.

Non esiste una lista tassativa di condotte illecite che possono costituire l’oggetto del whistleblowing. Si può tuttavia affermare che le condotte illecite oggetto delle segnalazioni meritevoli di tutela comprendono non solo l’intera gamma dei delitti previsti dal Modello 231, della prevenzione della corruzione ai sensi della norma ISO 37001, ma anche le situazioni in cui, nel corso dell’attività aziendale, si riscontri l’abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi indebiti, nonché i fatti/condotte che costituiscono violazione del codice etico aziendale idonei a esporre la compagine aziendale ad un rischio-reato⁴.

In particolare, la segnalazione può riguardare azioni od omissioni, commesse o tentate, che siano, anche alternativamente:

⁴ Si pensi, a titolo meramente esemplificativo, ai casi di uso distortivo dei fondi aziendali, demansionamenti, dichiarazioni non vere rese alla pubblica amministrazione per ottenere benefici altrimenti non spettanti, artefazione della documentazione aziendale archiviata suscettibile di rilevanza pubblica, assunzioni di favore (corruzione), operazioni finanziarie non supportate da idonea documentazione volte alla ricettazione o al riciclaggio di denaro o altri beni di provenienza delittuosa, violazione della concorrenza, violazione delle norme ambientali e di sicurezza sul lavoro, frode nelle pubbliche forniture, mendacità nelle qualità o quantità del prodotto o servizio reso, turbativa d’asta e alterazione di procedure di appalti, transazioni/negoziazioni senza delibera, Illegittima erogazione compensi incentivanti, Trattamenti di favore nei confronti di consulenti e professionisti.

- penalmente rilevanti;
- attuate in violazione del codice etico o di altre disposizioni-procedure aziendali, sanzionabili in via disciplinare;
- suscettibili di arrecare un indebito vantaggio all'azienda;
- suscettibili di arrecare un pregiudizio all'immagine dell'azienda e, conseguentemente, un danno reputazionale;
- suscettibili di arrecare un danno alla salute o sicurezza dei dipendenti e/o di arrecare un danno all'ambiente;
- riconducibili a condotte suscettibili di corruzione;
- illeciti relativi all'applicazione delle leggi e dei regolamenti 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;
- atti od omissioni che ledono gli interessi finanziari dell'Unione Europea (art. 325 del TFUE lotta contro la frode e le attività illegali che ledono gli interessi finanziari dell'Unione europea) come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'Unione europea;
- atti o omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE). Sono ricomprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, di imposta 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;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione europea nei settori indicati ai punti precedenti. In tale ambito vanno ricondotte, ad esempio, le pratiche abusive quali quelle definite dalla giurisprudenza della Corte di Giustizia dell'Unione europea.
- altri illeciti amministrativi, contabili, civili o penali;
- condotte illecite ai sensi del D.Lgs. n. 231/2001 e violazioni dei modelli di organizzazione, gestione e controllo adottati ai sensi dello stesso.

Coerentemente con l'ambito di applicazione del Decreto, è possibile quindi segnalare violazioni, inclusi fondati sospetti e condotte volte ad occultarle (ad esempio occultamento o distruzione di prove), di disposizioni normative nazionali o 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. Il Decreto non pregiudica l'applicazione di alcune disposizioni nazionali o dell'Unione Europea⁵.

⁵ In particolare, restano ferme le disposizioni nazionali o dell'Unione europea relative a: informazioni cosiddette "classificate" (ossia "riservate" ex Legge 124/2007); segreto professionale forense; segreto professionale medico; segretezza delle deliberazioni degli organi giurisdizionali; norme di procedura penale; autonomia e indipendenza della magistratura; difesa nazionale e di ordine e sicurezza pubblica; esercizio dei diritti dei lavoratori.

Si ricorda, inoltre, che l'art. 54 del D.Lgs. 165/2001 stabilisce, per i dipendenti pubblici, il divieto, già disciplinato nel codice etico aziendale, di chiedere o di accettare, a qualsiasi titolo, compensi, regali o altre utilità, in connessione con l'espletamento delle proprie funzioni o dei compiti affidati, fatti salvi i regali d'uso, purché di modico valore e nei limiti delle normali relazioni di cortesia.

Sono escluse dall'ambito di applicazione del Decreto e delle tutele ad esso correlate le seguenti tipologie di segnalazioni:

- contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate;
- segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali indicati nella parte II dell'allegato al Decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'Allegato al Decreto (a titolo esemplificativo e non esaustivo: segnalazioni di violazioni disciplinate in via obbligatoria nelle direttive e nei regolamenti dell'Unione europea e nelle disposizioni attuative dell'ordinamento italiano che già garantiscono apposite procedure di segnalazione);
- segnalazioni di violazioni in materia di sicurezza nazionale nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea.

Il whistleblowing non può in alcun caso avere ad oggetto questioni di carattere personale del segnalante, rivendicazioni o istanze attinenti alla disciplina del rapporto di lavoro o rapporti col superiore gerarchico o con i colleghi.

Si precisa che con riferimento alle segnalazioni relative a comportamenti personali ritenuti impropri ovvero alla violazione di norme etico-comportamentali sono attivi differenti canali di segnalazione disponibili nella intranet e/o nel sito istituzionale di Intellera.

MODALITÀ DI INOLTRO DELLE SEGNALAZIONI

Il D. Lgs 24/2023 prevede un sistema diversificato di presentazione delle Segnalazioni. Le stesse possono infatti essere effettuate attraverso:

1. canale interno
2. canale esterno
3. divulgazione pubblica
4. denuncia all'Autorità giudiziaria o contabile.

Laddove siano consentiti più canali, il canale da considerare in via primaria è il "canale interno". Come esplicitato nel seguito, infatti, solo per determinate tipologie di segnalazioni e subordinatamente al verificarsi di determinate condizioni, il segnalante può adire al "canale esterno", attivato presso l'Autorità Nazionale Anticorruzione (ANAC), oppure effettuare, sempre in via subordinata e al verificarsi di determinate condizioni, una divulgazione pubblica o una denuncia all'Autorità giudiziaria o contabile.

SEGNALAZIONI TRAMITE CANALE INTERNO

Il Canale implementato prevede l'utilizzo di uno strumento informatico dedicato (d'ora in poi anche la "Piattaforma"), che consente anche la possibilità di acquisizione di segnalazioni orali e anonime, come previsto dalla ISO 37001, effettuate attraverso sistemi di messaggistica vocale e distorsione della voce.

Tale Canale garantisce la riservatezza delle segnalazioni effettuate e della relativa documentazione (relativamente a identità del segnalante, persone coinvolte o persone comunque menzionate nella Segnalazione, nonché al contenuto della stessa) grazie al ricorso a strumenti di crittografia specifici della Piattaforma adottata. A tal fine la Piattaforma:

- prevede profili di accesso distinti per segnalante (intelleraconsulting.lumosplatform.com) e Comitato Whistleblowing (intelleraconsulting.lumosplatform.com/login);
- consente l'individuazione univoca delle segnalazioni e la loro tracciabilità nel tempo, attraverso apposita codifica;
- consente l'effettuazione di segnalazioni in forma anonima;
- consente l'effettuazione di segnalazioni in forma orale, con successiva possibilità di trascrizione previo consenso esplicito del segnalante;
- consente l'effettuazione di segnalazioni in forma orale e anonima, attraverso specifici meccanismi di distorsione della voce, con successiva possibilità di trascrizione previo consenso esplicito del segnalante;
- permette al segnalante di fornire informazioni circostanziate sui fatti e di allegare documentazione a supporto della segnalazione, integrando e modificando anche in momenti successivi le informazioni prodotte;
- consente al Comitato Whistleblowing di disporre di un'area riservata che permette la gestione delle segnalazioni ricevute, ivi incluse l'istruttoria e la storicizzazione delle informazioni;
- consente la comunicazione diretta tra segnalante e Comitato Whistleblowing attraverso l'utilizzo di chat collaborative, anche nel rispetto dell'anonimato;
- consente al segnalante di monitorare lo stato di avanzamento dell'istruttoria, anche attraverso apposite notifiche;
- consente al Comitato Whistleblowing di disporre di reportistica in merito alle segnalazioni ricevute e gestite, unitamente al relativo stato.

Le modalità operative di utilizzo della Piattaforma sono disponibili in allegato alla presente procedura ed è attivo l'utilizzo guidato accedendo alla stessa dalla intranet e dal sito istituzionale di Intellera.

REQUISITI DELLA SEGNALAZIONE

Ove si determini ad inoltrare una segnalazione, il segnalante ha il dovere di fornire tutti gli elementi utili a consentire al Comitato Whistleblowing di procedere alle dovute ed appropriate verifiche ed accertamenti per agevolarlo nel compito di riscontrare la fondatezza di quanto segnalato.

A tal fine, è opportuno che il segnalante fornisca al Comitato Whistleblowing quanti più tra gli elementi di seguito elencati (ove ciò sia possibile, tutti):

- le proprie generalità, salva l'ipotesi di segnalazioni anonime, con indicazione della posizione o funzione svolta nell'ambito dell'azienda;
- una chiara e completa descrizione dei fatti oggetto di segnalazione e delle circostanze in cui il segnalante ne è venuto a conoscenza;
- le circostanze di tempo e di luogo in cui i fatti oggetto di segnalazione sono stati commessi;
- le generalità dell'autore delle condotte illecite o delle irregolarità segnalate (o, in alternativa, altri elementi in grado di consentire l'identificazione del medesimo, quali ad esempio la qualifica rivestita o il servizio svolto in ambito aziendale);
- le generalità di eventuali altri soggetti che possono riferire sulle condotte illecite o sulle irregolarità segnalate (o, in alternativa, altri elementi in grado di consentire l'identificazione degli stessi, quali ad esempio la qualifica rivestita o il servizio svolto in ambito aziendale) e/o che siano potenzialmente a conoscenza dei fatti;
- l'allegazione di documenti a riprova di quanto segnalato (oppure, ove questi non siano nella disponibilità del segnalante, l'indicazione degli estremi degli stessi, del luogo ove siano custoditi o del soggetto che li detenga);
- ogni altra informazione che possa fornire un contributo utile all'attività di riscontro.

Non sono ricomprese tra le informazioni sulle violazioni segnalabili o denunciabili le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (cd. "voci di corridoio").

Qualora la segnalazione esuli dalle casistiche previste dalla norma per il whistleblowing, il Comitato Whistleblowing comunicherà al segnalante il rigetto della segnalazione per incompetenza a gestire la segnalazione.

Qualora la segnalazione contenga dati eccedenti, il Comitato Whistleblowing valuterà l'adozione delle più opportune iniziative volte alla cancellazione dei dati non pertinenti, se del caso chiedendo al segnalante l'eliminazione delle informazioni non necessarie per la gestione della segnalazione.

GESTIONE DELLE SEGNALAZIONI

Il Comitato Whistleblowing gestisce in autonomia e con garanzia di riservatezza le segnalazioni ricevute e valuta, sempre in autonomia e in conformità alle linee guida ISO 37008 già citata, la fondatezza delle segnalazioni ricevute e le eventuali azioni da intraprendere (a titolo esemplificativo, coinvolgimento delle Risorse Umane, del Collegio Sindacale, dell'Amministratore Delegato o del Consiglio di Amministrazione).

Il Comitato Whistleblowing deve, nel rispetto della riservatezza e garantendo l'imparzialità, effettuare ogni attività ritenuta necessaria al fine di valutare la fondatezza della segnalazione, avvalendosi, eventualmente, del supporto e della collaborazione delle competenti strutture aziendali e, all'occorrenza, di organi di controllo esterni (es. collegio sindacale), previo esplicito consenso del segnalante tramite chat in Piattaforma.

Nel caso in cui una segnalazione non risulti adeguatamente circostanziata, il Comitato Whistleblowing potrà richiedere al segnalante ulteriori elementi di dettaglio tramite chat in Piattaforma.

Nel caso in cui non si comprometta l'accertamento dei fatti, il segnalato potrà essere informato delle segnalazioni a suo carico; in ogni caso dovrà essere salvaguardato l'anonimato del segnalante.

Qualora ritenga la segnalazione non meritevole di approfondimento, il Comitato Whistleblowing ne dà comunicazione al segnalante.

Entro tre mesi dall'avviso di ricevimento della segnalazione o, in mancanza, entro tre mesi dalla scadenza del termine di sette giorni dalla segnalazione, il Comitato Whistleblowing fornisce riscontro al segnalante comunicando al segnalante in modo sintetico e tempestivo le determinazioni relative e/o conseguenti alla segnalazione.

Qualora ritenga la segnalazione meritevole di approfondimento, il Comitato Whistleblowing informa l'Amministratore Delegato (o il CdA nel caso in cui la segnalazione riguardi l'Amministratore Delegato o il Presidente Esecutivo).

Nel caso in cui la segnalazione dovesse risultare fondata, l'Amministratore Delegato provvederà a:

- 1) presentare denuncia all'autorità giudiziaria competente;
- 2) decidere i provvedimenti opportuni, inclusa l'eventuale azione disciplinare, nei confronti dell'autore della violazione, previa comunicazione al Responsabile di riferimento;
- 3) decidere in merito ai provvedimenti necessari a tutela di Intellera.

La segnalazione sarà senz'altro rigettata, con adeguata motivazione, e archiviata dal Comitato Whistleblowing al ricevimento delle segnalazioni nelle seguenti ipotesi:

- mancanza di interesse all'integrità aziendale;
- incompetenza dell'Organismo deputato al ricevimento delle segnalazioni;
- infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti;
- insussistenza dei presupposti di legge per l'esercizio delle vigilanze di competenza dell'OdV e/o Responsabile Anticorruzione (RAC);
- contenuto generico della segnalazione che non consente la comprensione dei fatti ovvero segnalazione di illeciti corredata da documentazione non appropriata o inconferente;
- produzione di sola documentazione in assenza di segnalazione di condotte illecite o irregolarità;
- mancanza di dati che costituiscono elementi essenziali della segnalazione.

Nella gestione delle segnalazioni è comunque garantita la riservatezza del contenuto e dell'identità del segnalante, ad eccezione dei seguenti casi:

- qualora ne venga accertata, anche con sentenza di primo grado, la responsabilità penale per i reati di calunnia o diffamazione o comunque per reati commessi con la segnalazione, ovvero la responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave;
- a fronte di richieste dell'Autorità Giudiziaria o altri aventi diritto.

Il Comitato Whistleblowing riporta periodicamente al Consiglio di Amministrazione della Società sul corretto funzionamento del sistema di whistleblowing e dà un'informativa almeno annuale dell'attività effettuata. Qualora si rilevino mancanze giudicate gravi, il Comitato

Whistleblowing potrà richiedere una convocazione straordinaria del Consiglio di Amministrazione per discutere degli opportuni interventi.

Qualora il segnalato coincida con uno dei membri del Comitato Whistleblowing la segnalazione deve essere tempestivamente portata all'attenzione dell'Amministratore Delegato che, con la collaborazione degli altri membri del Comitato Whistleblowing non oggetto della segnalazione, dopo le necessarie verifiche e approfondimenti, riferirà dell'accaduto alla prima riunione utile al Consiglio di Amministrazione. Per ulteriori dettagli si rinvia alla sezione Whistleblowing del MOG 231 della Società.

RISERVATEZZA DEL SEGNALANTE

All'atto del ricevimento della segnalazione i dati identificativi del segnalante, qualora presenti, saranno secretati per tutta la durata del procedimento volto ad accertare la fondatezza della segnalazione.

I dati forniti saranno trattati nell'ambito e nel rispetto della normativa applicabile e delle procedure aziendali, le quali prevedono, tra l'altro, la garanzia di riservatezza e la possibilità di utilizzare i dati acquisiti esclusivamente al fine di dar seguito alle segnalazioni, ivi inclusa l'adozione di eventuali provvedimenti disciplinari.

Le informazioni relative alle segnalazioni non possono essere utilizzate oltre quanto necessario per darne adeguato seguito.

L'identità del segnalante e qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente, tale identità non possono essere rivelate senza il consenso espresso del segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni. Perciò, nel caso in cui il Comitato Whistleblowing ritenga necessario, ai fini della gestione della segnalazione, il coinvolgimento di soggetti ad esso non appartenenti (es. consulenti, professionisti esterni, etc.), la comunicazione del nome del segnalante e/o di qualsiasi ulteriore informazione che possa consentire di risalire all'identità di tale soggetto è subordinata alla raccolta di un consenso scritto del segnalante, tramite piattaforma, a cura del Comitato Whistleblowing.

La violazione degli obblighi di riservatezza del segnalante, salvo quanto previsto ai sensi del D.Lgs. n. 24/2023, comporta la violazione di legge con la conseguente responsabilità disciplinare e irrogazione delle relative sanzioni. La trasmissione della segnalazione a soggetti interni a Intellera dovrà avvenire sempre previa eliminazione di tutti i riferimenti che consentano di risalire all'identità del segnalante e nel pieno rispetto dell'obbligo di riservatezza previsto dal D.Lgs. 24/2023.

Nell'ambito di un procedimento disciplinare, l'identità del segnalante può essere rivelata solo:

- con il consenso esplicito del segnalante;
- qualora la segnalazione risulti fondata e la conoscenza dell'identità del segnalante sia assolutamente necessaria alla difesa del segnalato.

L'anonimato del segnalante non è opponibile all'autorità giudiziaria; tuttavia, la segnalazione all'autorità giudiziaria deve avvenire evidenziando che essa è pervenuta da un soggetto cui è accordata la tutela della riservatezza.

I dati forniti in favore di chi dovesse esercitare i diritti di cui all'art.15 del GDPR 679/2016 non potranno contenere dati e/o informazioni che consentano di risalire al segnalante.

Coerentemente con quanto previsto dalla normativa di riferimento, deve essere garantita la riservatezza anche dei soggetti diversi dal segnalante, ma coinvolti nella segnalazione e beneficiari delle tutele previste dal Decreto, la cui identità dovrà essere mantenuta riservata dal Comitato Whistleblowing, salvo espresso obbligo a comunicare tali informazioni connesso all'applicazione di disposizioni normative o ove ottenuto l'espresso consenso dell'interessato.

Con riferimento al soggetto segnalato, la normativa non riconosce tuttavia il diritto di essere sempre informato della segnalazione che lo riguarda. Fa infatti eccezione al dovere di riservatezza delle persone coinvolte o menzionate nella segnalazione il caso in cui le segnalazioni siano oggetto di denuncia alle Autorità giudiziarie (ciò trova conferma nel fatto che il legislatore, nel prevedere la tutela della riservatezza nei procedimenti giudiziari, fa riferimento solo all'identità del segnalante e non anche a quella della persona coinvolta o menzionata nella segnalazione).

Nella gestione della Segnalazione dovranno in ogni caso essere adottate tutte le necessarie cautele al fine di evitare la indebita circolazione di informazioni personali, non solo verso l'esterno, ma anche all'interno dell'organizzazione.

CONSEGUENZE DELLE SEGNALAZIONI, DIVIETI E TUTELE

È vietato l'uso strumentale e/o improprio della segnalazione.

La normativa whistleblowing di cui al D.Lgs. 24/2023 riconosce specifiche tutele al segnalante e ad eventuali altri soggetti coinvolti nella segnalazione. I soggetti ai quali, in qualità di segnalanti, sono riconosciute le tutele dalla normativa whistleblowing⁶, sono:

- lavoratori subordinati, compresi lavoratori con contratto di lavoro a tempo parziale, intermittente, a tempo determinato, di somministrazione, di lavoro accessorio o che svolgono prestazioni occasionali;
- lavoratori autonomi⁷, collaboratori, liberi professionisti e consulenti che prestano servizi e/o opere per Intellera, anche qualora le modalità di esecuzione delle prestazioni siano realizzate mediante piattaforme digitali;
- tirocinanti e volontari, retribuiti e non retribuiti;

⁶ Affinché trovino applicazione le tutele rafforzate e specifiche previste dal Decreto, il segnalante deve dichiarare espressamente di voler beneficiare di tali tutele. Se la sua volontà non è desumibile dalla segnalazione, oppure essa è effettuata in forma anonima, detta segnalazione sarà considerata e trattata quale segnalazione ordinaria. In ogni caso, la Segnalazione sarà gestita come segnalazione ordinaria, quando essa sia effettuata da parte di un Segnalante appartenente ad un ente con una media di lavoratori inferiore a 50 e che non sia dotato di Modello ex D.Lgs. 231/2001.

⁷ Si tratta dei lavoratori autonomi indicati al capo I della L 81/2017; dei lavoratori con rapporti di lavoro autonomi disciplinati dal Titolo III del Libro V del Codice civile, ivi inclusi i contratti d'opera di cui all'art. 2222 del medesimo c.c.; i titolari di un rapporto di collaborazione di cui all'art. 409 del Codice di procedura civile. Ci si riferisce anche ai rapporti di agenzia, di rappresentanza commerciale ed altri rapporti di collaborazione che si concretizzano in una prestazione di opera continuativa e coordinata, prevalentemente personale, anche se non a carattere subordinato: a titolo esemplificativo avvocati, ingegneri e altri professionisti che prestano la loro attività lavorativa per un soggetto del settore privato organizzandosi autonomamente (rapporto parasubordinato); i titolari di un rapporto di collaborazione di cui all'art. 2 del D.Lgs. n. 81/2015, cioè collaborazioni organizzate dal committente che si concretizzano in prestazioni di lavoro esclusivamente personali e continuative, le cui modalità di esecuzione siano organizzate dal committente.

- azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.

Le tutele sono inoltre riconosciute, oltre ai suddetti soggetti che effettuano segnalazioni, anche a coloro che potrebbero essere destinatari di ritorsioni, intraprese anche indirettamente, in ragione del ruolo assunto nell'ambito del processo di segnalazione e/o del particolare rapporto che li lega al segnalante. Tali soggetti godono di tutela analoga a quella del segnalante e sono:

- facilitatori, ossia persone fisiche che assistono eventualmente il segnalante nel processo di segnalazione, operanti all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- persone del medesimo contesto lavorativo del segnalante e che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado;
- colleghi di lavoro del segnalante che lavorano nel medesimo contesto lavorativo dello stesso e che hanno con il segnalante un rapporto abituale e corrente;
- enti di proprietà del segnalante o per i quali lo stesso lavora nonché enti che operano nel medesimo contesto lavorativo del segnalante.

Si precisa che la tutela dei segnalanti si applica anche qualora la segnalazione avvenga:

- 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 medesimo.

Il codice sanzionatorio adottato nell'ambito del MOG 231/2001, cui si rinvia per dettagli e approfondimenti, sanziona l'uso strumentale e/o improprio della segnalazione.

Allo stesso modo, il codice sanzionatorio tutela la segnalazione fondata e pertinente con i principi ispiratori dell'istituto; onde nessuno potrà essere licenziato o, ancora, subire ritorsioni o demansionamenti in conseguenza di un uso lecito e pertinente della segnalazione.

Chiunque segnali, sussistendone le condizioni di cui agli articoli 6⁸ e 16⁹ del D.Lgs. 24/2023, o denunci all'autorità giudiziaria ordinaria o a quella contabile condotte illecite di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione.

Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del Codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante.

Non è tollerata alcuna forma di ritorsione o misure discriminatorie nei confronti del dipendente che effettua una segnalazione. Tra le misure discriminatorie vanno ricomprese misure disciplinari, molestie o ritorsioni che determinino condizioni di lavoro inaccettabili. Il dipendente che ritiene di essere oggetto di misure discriminatorie a seguito di una segnalazione può informare il Comitato Whistleblowing che riporterà all'organo amministrativo

⁸ Condizioni per l'effettuazione della segnalazione esterna.

⁹ Condizioni per la protezione della persona segnalante.

cui compete, ove confermate le misure discriminatorie, ripristinare le normali condizioni di lavoro.

L'adozione di misure ritenute ritorsive nei confronti del segnalante può essere comunicata all'ANAC (Autorità Nazionale AntiCorruzione) dall'interessato o, eventualmente, dalle organizzazioni sindacali maggiormente rappresentative, ove presenti nell'organizzazione nella quale le stesse sono state realizzate.

La violazione delle disposizioni di legge determina l'applicazione di sanzioni pecuniarie, nonché delle ulteriori sanzioni previste ex lege per la condotta illecita posta in essere.

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Qualora un dipendente ritenga di aver subito uno dei già menzionati comportamenti a causa dell'inoltro di una segnalazione, potrà comunicarlo ai canali attivati dalla funzione People Workplace Experience e/o all'Ethics Task Force che si attiveranno per l'analisi del caso e le azioni successive.

Per le conseguenze connesse all'eventuale adozione di atti ritorsivi e/o discriminatori, diretti o indiretti, compiuti nei confronti del segnalante-dipendente per motivi collegati, anche indirettamente, alla segnalazione e per la relativa disciplina delle sanzioni adottabili si rinvia alla specifica sezione del Modello Organizzativo 231/2001 di Intellera.

RESPONSABILITÀ DEL SEGNALANTE

La presente procedura lascia inalterata la responsabilità penale nel caso di segnalazioni calunniose o diffamatorie. Quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele di cui al D.Lgs. n. 24/2023 non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare.

La tutela del segnalanti non trova applicazione in caso di responsabilità penale (calunnia o diffamazione) o civile (danno ingiusto causato da dolo o colpa).

Al lavoratore dipendente di Intellera effettuati con dolo o colpa grave segnalazioni che si rivelano infondate, si applicano le misure sanzionatorie previste nel Codice sanzionatorio del Modello 231 aziendale (Parte generale) modulate in proporzione alla gravità e secondo i criteri generali lì descritti.

TRATTAMENTO DEI DATI PERSONALI

La gestione delle segnalazioni deve avvenire in conformità alla normativa in tema di tutela dei dati personali. Si precisa che i professionisti individuati per la gestione della segnalazione (Comitato Whistleblowing) operano quali soggetti autorizzati al trattamento dei dati personali, ai sensi degli articoli 29 e 32, comma 4, GDPR nonché dell'articolo 2-quaterdecies, DLgs. 196/2003 ("Codice Privacy"). Per dettagli si rinvia all'informativa e ai moduli di consenso allegati alla presente procedura.

Nella gestione delle Segnalazioni, il Titolare del trattamento e ciascun membro del Comitato Whistleblowing, nell'ambito dei rispettivi ruoli e responsabilità, sono tenuti ad osservare i seguenti principi fondamentali, comunicando prontamente eventuali anomalie o situazioni di non conformità:

- le informazioni di natura personale (di seguito anche "Dati") dei soggetti interessati devono essere trattate in modo lecito, corretto e trasparente nei confronti dei soggetti interessati, in conformità alle disposizioni normative in materia di protezione dei dati personali e di ogni ulteriore normativa applicabile;
- i Dati devono essere raccolti e trattati unicamente al fine di gestire e dare seguito alle segnalazioni;
- possono essere raccolti e utilizzati unicamente i Dati ritenuti adeguati, pertinenti e utili per la gestione della segnalazione. A tal riguardo, i dati personali che manifestamente non sono utili per la gestione di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, devono essere cancellati. Pertanto, qualora la segnalazione contenga informazioni eccedenti, il Comitato Whistleblowing valuterà l'adozione delle più opportune iniziative volte alla cancellazione dei Dati non pertinenti, se del caso chiedendo al segnalante l'eliminazione delle informazioni da esso fornite e ritenute non necessarie per la gestione della segnalazione;
- i Dati devono essere esatti e, se necessario, aggiornati. A tale proposito, devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti relativi alla specifica segnalazione. Anche in questo caso, ove possibile, tali interventi possono essere svolti in coordinamento con il soggetto segnalante;
- i Dati devono essere conservati con modalità e strumenti che consentano l'identificazione degli interessati solo per il tempo necessario al trattamento della specifica segnalazione e in ogni caso nel rispetto delle tempistiche definite dalla legge;
- i Dati devono essere cancellati, tramite processi manuali o automatizzati dai componenti del Comitato Whistleblowing, non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione;
- il trattamento deve essere eseguito ricorrendo a idonei strumenti di protezione dei dati personali, quali la crittografia e ulteriori misure tecniche e organizzative atte a prevenire la perdita, la distruzione, l'accesso e l'uso non autorizzato;
- il Titolare, eventualmente anche su iniziativa del Comitato Whistleblowing, dispone periodicamente il riesame e l'aggiornamento delle misure di sicurezza adottate;
- il rischio del trattamento deve essere esaminato dal Titolare del trattamento tramite la redazione e il periodico aggiornamento di una valutazione d'impatto sulla protezione dei Dati, ai sensi dell'articolo 35, GDPR;
- gli interessati (ad es. segnalanti, facilitatori, etc.) ricevono l'informativa sul trattamento dei dati personali ai sensi degli articoli 13 e 14, GDPR, tramite la piattaforma utilizzata per la gestione delle segnalazioni; tale documento indica anche le modalità di esercizio dei diritti degli interessati riconosciuti dal GDPR;
- nel caso in cui il Comitato ritenga necessario, ai fini della gestione della segnalazione, il coinvolgimento di terzi (soggetti estranei al Comitato) deve essere favorita la condivisione di dati e informazioni con modalità che consentano di preservare l'anonimato di tutti i soggetti coinvolti. La comunicazione a soggetti terzi del nome del segnalante e/o di qualsiasi ulteriore informazione che possa consentire di risalire all'identità di tale soggetto è subordinata alla raccolta di un consenso scritto del

segnalante a cura dei membri del Comitato Whistleblowing; il Titolare del trattamento, per il tramite della Funzione Privacy, censisce il trattamento in questione nel Registro delle attività di trattamento previsto dall'articolo 30 GDPR, tenuto conto delle informazioni connesse a quelle di acquisizione e gestione delle segnalazioni;

- anche attraverso le caratteristiche dello strumento utilizzato, non deve essere possibile il tracciamento del segnalante al canale di segnalazione, dovendo essere individuabile l'identità del segnalante unicamente dalle informazioni fornite e autorizzate dallo stesso;
- deve essere ripercorribile l'attività svolta dai componenti del Comitato Whistleblowing (per tutto il tempo di conservazione dei dati della Segnalazione), al fine di evitare l'uso improprio di Dati relativi alla segnalazione.

MONITORAGGIO

Il numero di segnalazioni ricevute e il relativo stato di avanzamento sono comunicate con cadenza almeno annuale al Consiglio di Amministrazione.

I dati ottenuti mediante le segnalazioni e le successive istruttorie dovranno essere utilizzati per aggiornare o integrare la Matrice di rischio 231 e il Piano anticorruzione ai sensi della ISO 37001.

CONSERVAZIONE DELLE SEGNALAZIONI

Le segnalazioni 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.

SEGNALAZIONE ESTERNA

L'art. 3, comma 2, lett. b), del D.Lgs. n. 24/2023, nel caso di ente che abbia adottato il Modello 231 e abbia anche impiegato, nell'ultimo anno di attività, una media di 50 o più dipendenti, prevede non solo la possibilità per i segnalanti di fare ricorso al canale di segnalazione esterna e alle divulgazioni pubbliche, ma richiama in aggiunta la facoltà di segnalare comportamenti contrari, oltre che al D.Lgs. 231/2001 e al Modello organizzativo, anche al diritto dell'Unione e agli atti dell'UE indicati nell'allegato al decreto. Nel caso di Intellera sono possibili:

	Segnalazioni di ogni illecito amministrativo, contabile, civile o penale	Segnalazioni afferenti la violazione di ogni documento di cui al MOG 231 (codice etico, policies etc.)	Segnalazioni di atti in violazione o omissioni contrari al diritto UE indicati nell'allegato al D.Lvo n. 24/2023	Accesso al canale esterno ANAC di segnalazione e tutele in caso di divulgazioni pubbliche
Soggetti del settore privato con almeno 50 dipendenti e con il MOG 231	NO	SI	SI	SI

Resta inteso che il segnalante potrà avvalersi di tutti i canali di segnalazione, sia interni – comunque predisposti in conformità al decreto legislativo n. 24/2023 – che esterni.

In tale ultimo caso, il segnalante può procedere alla segnalazione esterna, avvalendosi del canale di segnalazione appositamente creato dall'ANAC¹⁰, laddove ricorra uno dei seguenti requisiti:

¹⁰ Il canale esterno gestito dall'ANAC è usufruibile accedendo dal sito istituzionale dell'Autorità al servizio dedicato al "whistleblowing" (<https://www.anticorruzione.it/-/whistleblowing>). Analogamente al canale interno, il canale esterno

- il canale di segnalazione interno predisposto dalla società non è attivo o non è correttamente funzionante;
- è stata già effettuata una segnalazione interna che non ha avuto seguito;
- il segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare un rischio di ritorsione;
- il segnalante ha fondati motivi di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le segnalazioni esterne possono essere effettuate attraverso piattaforma informatica predisposta dall’Autorità, telefono, sistemi di messaggistica vocale o, su richiesta del segnalante, incontri diretti.

L’ANAC, ai sensi dell’art. 21 del D.Lgs. 24/2023, applica al responsabile le seguenti sanzioni amministrative pecuniarie:

- a) da 10.000 a 50.000 euro 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 di cui all’articolo 12 del Decreto;
- b) 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;
- c) da 500 a 2.500 euro, nel caso in cui venga accertata la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia.

DIVULGAZIONE PUBBLICA

Attraverso una divulgazione pubblica, il segnalante rende le informazioni sulle violazioni di pubblico dominio tramite la stampa o mezzi elettronici o comunque attraverso mezzi di diffusione in grado di raggiungere un numero elevato di persone. In tale circostanza, la protezione del segnalante è tuttavia riconosciuta solo nel caso in cui al momento della divulgazione ricorra almeno una delle seguenti condizioni:

- ad una segnalazione interna, a cui non è stato dato riscontro in merito alle misure previste/adottate o nei tempi previsti, ha fatto seguito una segnalazione esterna ad ANAC, la quale, a sua volta, non ha fornito riscontro al segnalante entro termini ragionevoli¹¹;
- è stata effettuata una segnalazione esterna direttamente all’ANAC che, tuttavia, non ha dato riscontro al segnalante in merito alle misure previste o adottate per dare seguito alla segnalazione entro termini ragionevoli;
- sulla base di motivazioni ragionevoli e fondate alla luce delle circostanze, il segnalante ritenga che la violazione possa rappresentare un pericolo imminente o palese per il pubblico interesse o possa comportare il rischio di ritorsioni oppure possa non avere efficace seguito.

garantisce la riservatezza dei soggetti coinvolti nonché del contenuto della segnalazione e della relativa documentazione.

¹¹ Tre mesi o, se ricorrono giustificate e motivate ragioni, sei mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei sette giorni dal ricevimento.

Nella divulgazione pubblica, dove il Segnalante riveli volontariamente la propria identità, non rileva la tutela della riservatezza, ferme restando tutte le altre forme di protezione previste per il segnalante.

DENUNCIA ALL'AUTORITÀ GIUDIZIARIA O CONTABILE

Il D.Lgs. 24/2023 riconosce ai soggetti tutelati anche la possibilità di rivolgersi alle Autorità giudiziarie o contabili per inoltrare una denuncia di condotte illecite di cui siano venuti a conoscenza nel contesto lavorativo. A tale proposito si precisa che, qualora il segnalante rivesta la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, anche laddove lo stesso abbia effettuato una segnalazione attraverso i canali interni o esterni previsti dal Decreto, ciò non lo esonera dall'obbligo di denunciare alla competente Autorità giudiziaria o contabile i fatti penalmente rilevanti e le ipotesi di danno erariale, in merito a reati procedibili d'ufficio.

I presidi sulla tutela della riservatezza e del contenuto delle segnalazioni sono applicati anche dalle Autorità giudiziarie o contabili cui è sporta la denuncia.

6. STANDARD E STRUMENTI DI RIFERIMENTO

STANDARD E STRUMENTI DI RIFERIMENTO

1. Manuale d'uso della Piattaforma Whistleblowing
2. Informativa Whistleblowing
3. Raccolta consenso per condivisione a terzi
4. Raccolta consenso per registrazione o trascrizione della segnalazione