Impianto di Arcore (MB) – 20862 Via Achille Grandi, 70 Tel: 039/6755344
Impianto di Settimo Milanese (MI) – 20019 Via A. Sabin, 28 Tel: 02/33599133
Impianto di Senago (MI) – 20030 Viale Europa, 17 Tel: 02/49580470

Member of CISQ Federation
CERTIFIED MANAGEMENT SYSTEM ISO 14001

15.12.2023 REV. 00

PROCEDURA WHISTLEBLOWING

La presente procedura viene adottata da Tao Ambiente Srl (di seguito la Società) allo scopo di disciplinare l'organizzazione nell'applicazione del sistema di segnalazioni di irregolarità nell'ambito dell'attività svolta dalla Società. **La presente procedura è parte integrante del Modello Organizzativo della Società ai sensi del D. Lgs. N.231/2001.**

INDICE

INTRODUZIONE
1. **AMBITO DI APPLICAZIONE**
   - **1.1 Ambito soggettivo di applicazione: i destinatari della nuova disciplina**
   - **1.2 Ambito oggettivo di applicazione**
2. **IL SEGNALATORE / WHISTLEBLOWER**
   - **2.1 Soggetti legittimati a presentare le segnalazioni**
3. **DEFINIZIONE CONTENUTO DELLE SEGNALAZIONI**
   - **3.1 Definizioni**
   - **3.2 Contenuto**
   - **3.3 Esclusioni**
4. **CANALI DI SEGNALAZIONE**
   - **4.1 Canale interno di segnalazione**
   - **4.2 Strumenti di segnalazione**
   - **4.3 Requisiti**
   - **4.4 Istituzione tramite delibera specifica**
   - **4.5 Informativa alle rappresentanze sindacali**
5. **LA GESTIONE OPERATIVA DELLE SEGNALAZIONI**
   - **5.1 Canali in forma scritta**
   - **5.2 Canali in forma orale**
   - **5.3 Canali in forma orale con incontro diretto**
   - **5.4 Ricezione della segnalazione**
   - **5.5 La procedibilità della segnalazione**
   - **5.6 L'ammissibilità della segnalazione**
   - **5.7 Istruttoria e accertamento della segnalazione**
   - **5.8 Riscontro al segnalante**
6. **LA TUTELA DEL SEGNALANTE E DEI SOGGETTI AD ESSO ASSIMILATI**
   - **6.1 La riservatezza dell'identità del segnalante**
   - **6.2 il divieto e la protezione contro le ritorsioni**
   - **6.3 La limitazione di responsabilità del segnalante**
7. **TRATTAMENTO DEI DATI PERSONALI**
   - **7.1 Il ricevimento e la gestione di una segnalazione**
   - **7.2 Impostazione ed esecuzione dei trattamenti conseguenti alle segnalazioni**
8. **SISTEMA SANZIONATORIO**
9. **DISCIPLINA WHISTLEBLOWING E MODELLO ORGANIZZATIVO**
10. **ATTIVITA DI FORMAZIONE E INFORMAZIONE**
11. **SEGNALAZIONE ESTERNA E DIVULGAZIONE PUBBLICA**
    - **11.1 Le condizioni per la segnalazione esterna**
    - **11.2 La procedura della divulgazione pubblica**

INTRODUZIONE

Con il Decreto Legislativo 10 marzo 2023 n. 24, pubblicato sulla G.U. il 15 marzo 2023, è stata recepita nell'ordinamento italiano la direttiva UE 2019/1937, riguardante "**la protezione delle persone che segnalano violazioni del diritto dell'Unione"** (c.d. disciplina whistleblowing).
La normativa riguarda sia il settore pubblico che quello privato e introduce una regolamentazione in materia di protezione delle persone che segnalano violazioni di illeciti.
L'obiettivo della direttiva europea è quello di stabilire norme minime comuni per garantire un elevato livello di protezione delle persone che segnalano violazioni del diritto dell'Unione, creando canali di comunicazione sicuri sia all'interno dell'organizzazione sia all'esterno.

1. AMBITO DI APPLICAZIONE

1.1 Ambito soggettivo di applicazione: i destinatari della nuova disciplina

I destinatari della disciplina sono i soggetti pubblici e i soggetti privati (artt. 2 e 3).
Per quanto riguarda i soggetti del settore privato, sono sottoposti alla disciplina:

- i soggetti che hanno impiegato, nell'ultimo anno, la media di almeno 50 lavoratori subordinati con contratti sia a tempo indeterminato che determinato;
- i soggetti che nell'ultimo anno non hanno raggiunto la media di 50 lavoratori subordinati, ma operano nei servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e del finanziamento del terrorismo, nonché della sicurezza dei trasporti;
- **tutti i soggetti, diversi dal punto precedente, ma dotati del modello di organizzazione, gestione e controllo, ai sensi del D.LGS.231/2001, anche se non hanno raggiunto i 50 lavoratori.**

1.2 Ambito oggettivo di applicazione

Dal punto di vista oggettivo la norma si applica alle violazioni delle disposizioni normative nazionali e dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui i soggetti segnalanti siano venuti a conoscenza in un contesto lavorativo (art.1).

Violazioni delle disposizioni normative nazionali

- illeciti penali, civili, amministrativi o contabili diversi rispetto a quelli specificamente individuati come violazioni del diritto UE, come sotto definite;
- reati presupposto per l'applicazione del Decreto 231;
- violazioni dei modelli di organizzazione e gestione previsti nel citato Decreto 231, anch'esse non riconducibili alle violazioni del diritto dell'UE come sotto definite.

Violazioni della normativa europea

Si tratta di:

- illeciti commessi in violazione della normativa dell'UE indicata nell'Allegato 1 al Decreto e di tutte le disposizioni nazionali che ne danno attuazione. Si tratta di illeciti dei settori: contratti 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'UE) come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE.

- atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali. Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposta sulle imprese 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 imprese;
- 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 definite dalla giurisprudenza della Corte di Giustizia dell'Ue.

Invece, per quanto riguarda il settore privato, le segnalazioni possono avere a oggetto violazioni della disciplina nazionale solo con riferimento ai reati 231 e alle violazioni del modello organizzativo 231, nonché quelle riguardanti il diritto europeo nelle materie sopra indicate.

2. IL SEGNALATORE / WHISTLEBLOWER

Il segnalatore è la persona fisica che segnala o divulga informazioni sulle violazioni, acquisite nell'ambito della sua attività professionale, a prescindere dalla natura di tale attività o dal fatto che il rapporto di lavoro sia nel frattempo terminato o non ancora iniziato.

2.1. Soggetti legittimati a presentare le segnalazioni

Il segnalatore può essere un lavoratore dipendente o autonomo, possono essere lavoratori con contratti atipici, a tempo parziale, determinato, indeterminato o assunto tramite un'agenzia interinale, tirocinanti o volontari, consulenti, subappaltatori, fornitori, personale che ricopre funzioni direttive, azionisti.
Per godere delle misure di protezione sono stabiliti specifici requisiti:

- il segnalatore deve avere ragionevoli motivi, alla luce delle circostanze e delle informazioni di cui dispone al momento della segnalazione, per ritenere che i fatti che segnala siano veri;
- Il segnalatore abbia fondati motivi per ritenere che le informazioni segnalate, rientrino nell'ambito di applicazione della direttiva stessa.

La direttiva estende le misure di protezione anche ai cosiddetti "facilitatori", ossia coloro che assistono il segnalante nel processo di segnalazione, sono estese ai terzi connessi con il segnalante, quali ad esempio colleghi, famigliari o i soggetti giuridici collegati con il segnalante.

3. DEFINIZIONE CONTENUTO DELLE SEGNALAZIONI

3.1 Definizioni

Le segnalazioni sono definite come le informazioni, compresi i fondati sospetti su violazioni già commesse o non ancora commesse (ma sulla base di elementi concreti potrebbero esserlo) nonché su condotte volte ad occultare, (ad esempio occultamento o distruzione di prove).

3.2 Contenuto delle segnalazioni

Le segnalazioni devono essere **circostanziate**, al fine di consentire la valutazione dei fatti.
E' necessario che risultino chiari i seguenti elementi della segnalazione:

- **i dati identificativi del segnalante** (nome, cognome, luogo e data di nascita) e un recapito a cui verranno comunicati i successivi aggiornamenti;
- **le circostanze di tempo e di luogo** in cui si è verificato il fatto e una descrizione dei fatti specificando i dettagli e la modalità in cui si è venuti a conoscenza dei fatti stessi;
- **le generalità** o altri elementi per consentire di identificare il soggetto cui attribuire i fatti segnalati.

In caso di utilizzo di canale analogico (piattaforma messa a disposizione dall'azienda) il segnalante deve indicare espressamente di voler beneficiare delle **tutele in materia whistleblowing** (inserendo la dicitura "riservata al gestore delle segnalazioni").
E' utile allegare alla segnalazione documenti che possono fornire elementi di fondatezza dei fatti, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

3.3 Esclusioni

Sono escluse le segnalazioni:

- di contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale del segnalante che attengono ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate; (vertenze di lavoro, conflitti interpersonali tra colleghi).
- In materia di sicurezza nazionale;
- le violazioni già regolamentate in via obbligatoria di settori speciali, ove si continuano ad applicare le segnalazioni ad hoc (servizi finanziari, prevenzione riciclaggio, sicurezza dei trasporti, tutela dell'ambiente).

4. CANALI DI SEGNALAZIONE

Il Decreto riserva una grande importanza ai canali di segnalazione, i quali sono:

- il canale interno alla società;
- canale esterno alla società istituito e gestito dall'ANAC;
- la divulgazione pubblica (da usare in extrema ratio)
- la denuncia all'autorità giudiziaria e contabile.

Le linee guida ANAC ribadiscono una gradualità di scelta del canale di segnalazione.
Si specifica che:

- per gli enti privati che **non hanno raggiunto la media di 50 lavoratori e hanno adottato il modello organizzativo 231, le segnalazioni devono riguardare solo condotte illeciti rilevanti inerenti alla disciplina 231, o, violazioni del modello 231 e devono essere effettuate unicamente attraverso il canale interno;**
- per gli enti che hanno impiegato la media di 50 lavoratori e hanno adottato il modello organizzativo 231 le segnalazioni possono:
  - avere ad oggetto condotte illecite o violazioni del modello organizzativo 231 ed essere effettuate solo attraverso canale interno;
  - avere ad oggetto violazioni del diritto UE ed essere effettuate tramite tutti i canali sopra riportati.

4.1 Canale interno di segnalazione

Ai sensi dell'Art. 4 del Decreto La Società ha attivato il seguente canale di segnalazione interna che, tramite specifica piattaforma, consente l'invio in modalità informatica le segnalazioni in forma scritta e garantisce, anche tramite strumenti di crittografia, la riservatezza dell'identità del segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione:

Piattaforma SCS Whistleblowing: link: **https://scswhistleblowing.com/taoambientesrl/form**

La piattaforma è accessibile attraverso il sito web della Società: TAO AMBIENTE SRL
Lo strumento risponde ai requisiti di sicurezza, ed è conforme alla norma in materia di protezione dei dati personali, che sono conservati e archiviati in modo sicuro da Reevo (Società italiana con sede e server in Italia, certificata ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISAE 3402 e SSAE18).

A difesa della piattaforma SCS Whistleblowing sono attivi sistemi di protezione firewall nonché sistemi finalizzati a mitigare attacchi DDOS. Vengono inoltre eseguiti periodicamente Penetration Test.. Gli elevati standard sono garantiti da periodici audit curati da enti terzi.
È consentito effettuare Segnalazioni Whistleblowing sia ORDINARIE CHE ANONIME.
Si segnala che la piattaforma consente la possibilità per il segnalante di restare in contatto con il gestore della segnalazione durante la gestione della segnalazione anonima, potendo fornire chiarimenti e/o integrazioni documentali attraverso un sistema di messaggistica che ne garantisce l'anonimato.
Nondimeno, occorre tenere conto che l'invio di una segnalazione whistleblowing anonima potrebbe rendere più difficoltoso l'accertamento della condotta segnalata e le interlocuzioni tra il gestore e segnalante e quindi inficiare l'utilità della segnalazione stessa.

4.2 Strumenti di segnalazione

Per quanto attiene gli strumenti per effettuare le segnalazioni, l'articolo 4 del decreto prevede che la segnalazione possa essere fatta:

- In forma scritta analogica o con modalità informatiche;
- In forma orale attraverso linee telefoniche dedicate,
- messaggistica vocale,
- su richiesta del segnalante, con un incontro diretto con il gestore della segnalazione, che deve essere fissato in un tempo ragionevole,

Per l'impresa **è obbligatorio** predisporre sia il canale scritto (analogico o informatico) che quello orale, mettendoli entrambi a disposizione del segnalante.
Per la modalità scritta ANAC suggerisce di inserire la segnalazione in due buste chiuse includendo nella prima i dati identificativi del segnalante, inserendo un documento d'identità. Nella seconda l'oggetto della segnalazione. Entrambe le buste dovranno essere inserite in una terza busta riportando all'esterno la dicitura "riservata al gestore della segnalazione".

4.3 Requisiti

Il canale di segnalazione interna è idoneo ad assicurare la riservatezza dell'identità del segnalante e delle persone coinvolte (segnalatore, facilitatore, eventuali altri terzi), del contenuto della segnalazione e della documentazione a essa relativa.
La gestione delle segnalazioni è stata affidata all'Organismo di Vigilanza 231 (OdV) della società, soggetto dotato di competenze tecniche, di autonomia, indipendenza e imparzialità.

Per le segnalazioni in forma scritta si dovranno inoltrare tramite piattaforma online SCS Whistleblowing link: https://scswhistleblowing.com/taoambientesrl/form o raccomandata cartacea a OdV, tramite il seguente indirizzo Diade Srl via delle Robinie, 4 20065 Inzago (Mi) nella persona del Dr Saverio Da Pozzo.
Per le segnalazioni tramite forma orale tramite l'incontro diretto con il gestore della segnalazione OdV Diade Srl via delle Robinie, 4 20065 Inzago (Mi) nella persona del Dr Saverio Da Pozzo. Oppure con messaggistica vocale registrata link: link https://scswhistleblowing.com/taoambientesrl/form

4.4 Istituzione tramite delibera specifica

Gli enti, sentite le rappresentanze o le organizzazioni sindacali, hanno l'onere di definire in un **apposito atto organizzativo** le procedure per il ricevimento delle segnalazioni e per la loro gestione. Tale atto deve essere adottato con **delibera dell'organo amministrativo.**

4.5 Informativa alle rappresentanze sindacali

Ai sensi dell'art 4 del Decreto, l'azienda ha comunicato alle organizzazioni sindacali il recepimento del Decreto 24/2023, l'adozione di idonei canali interni per le segnalazioni, la redazione della procedura whistleblowing, pubblicata sul sito internet, e distribuita a tutto il personale.
Ha altresì comunicato che il ruolo di gestore delle segnalazioni è rappresentato dall' OdV 231.

5. LA GESTIONE OPERATIVA DELLE SEGNALAZIONI

Il decreto disciplina la gestione del canale di segnalazione prevedendo apposite procedure.

5.1 Canali in forma scritta:

1. **Segnalazione mediante Posta ordinaria (lettere raccomandate)**

Al momento della ricezione, il gestore della segnalazione:

- garantisce la riservatezza dell'identità del segnalante e del contenuto delle buste;
- procede all'archiviazione della segnalazione attraverso idonei strumenti che permettano di garantire la riservatezza in archivi protetti.

2. **Utilizzo piattaforma informatica (SCS Whistleblowing)**

La segnalazione inviata viene indirizzata al gestore della segnalazione garantendo, anche grazie a strumenti di crittografia E2E, la riservatezza delle persone, delle segnalazioni e della relativa documentazione.

5.2 Canali in forma orale (linee telefoniche o sistemi di messaggistica vocale)

- Nel caso si utilizzi una linea telefonica il personale addetto documenta mediante resoconto dettagliato del messaggio e il contenuto deve essere controfirmato dal segnalante, previa verifica ed eventuale rettifica del contenuto. Del riscontro sottoscritto viene fornita copia al segnalante.
- La piattaforma adottata dall'azienda mette a disposizione la modalità di registrazione vocale che permette la registrazione del messaggio del segnalante. Questa verrà conservata dal gestore della segnalazione, previo consenso del segnalante, all'interno di un dispositivo idoneo alla conservazione e all'ascolto.

5.3 Canali in forma orale con incontro diretto

È prevista la possibilità che il whistleblower richieda un incontro presso gli uffici o alla persona deputata alla gestione della segnalazione. In questo caso l'impresa deve garantire lo svolgimento dell'incontro entro un tempo ragionevole di 10/15 giorni.

L'incontro avverrà in un luogo che garantisca la riservatezza del segnalante. Previo consenso del segnalante. E' consigliato effettuare una registrazione. Se non è possibile effettuare la registrazione occorre stilare un verbale che dovrà essere sottoscritto dal segnalante e da chi ha ricevuto la segnalazione.

5.4 Ricezione della segnalazione

Se il segnalante sceglie di utilizzare il canale mediante piattaforma, all'apertura della segnalazione gli verrà assegnato un ticket che permette al segnalante di entrare nella pagina dedicata e monitorare l'avanzamento della sua segnalazione.

In caso di segnalazione tramite posta raccomandata il gestore della segnalazione deve rilasciare al segnalante l'avviso di ricezione entro sette giorni dalla presentazione della segnalazione.

L'avviso verrà inviato al recapito indicato dal segnalante. In assenza di recapito del segnalante non si potrà interagire e si potrà considerare la segnalazione come non gestibile, ai sensi della disciplina whistleblowing. (Lasciando traccia della segnalazione)

Nel caso di segnalazioni anonime, se le stesse risultino puntuali, circostanziate e supportate da idonea documentazione, saranno equiparate alle segnalazioni ordinarie e trattate. In ogni caso le segnalazioni anonime dovranno essere registrate e la documentazione conservata.

Qualora la segnalazione venisse presentata ad un soggetto diverso da quello individuato e sia evidente che si tratti di whistleblowing la stessa deve essere trasmessa entro sette giorni dal ricevimento al soggetto interno competente, senza trattenerne copia dandone notizia al segnalante.

5.5 La procedibilità della segnalazione

Per potere dare corso al procedimento, il gestore della segnalazione dovrà come prima cosa verificare la sussistenza dei presupposti soggettivi e oggettivi e che il segnalante sia soggetto legittimato ad effettuare la segnalazione e che l'oggetto della segnalazione rientri nell'ambito di applicazione.

5.6 L'ammissibilità della segnalazione

Ai fini dell'ammissibilità come segnalazione whistleblowing è necessario che risultino chiare:

- **La circostanza di tempo e di luogo** in cui si è verificato il fatto con una descrizione dei fatti oggetto della segnalazione, una descrizione dei fatti con dettagli relativi alle notizie circostanziali e ove presenti, le modalità attraverso cui il segnalante è venuto a conoscenza dei fatti.
- **Le generalità o altri elementi** che consentono di identificare il soggetto a cui attribuire i fatti.

Alla luce di queste indicazioni una segnalazione può essere ritenuta inammissibile per:

- mancanza di dati che costituiscono gli elementi essenziali nella segnalazione;
- manifesta infondatezza degli elementi riconducibili alle violazioni tipicizzate dal legislatore;
- esposizione generica dei fatti tale da non consentirne la comprensione;
- produzione di sola documentazione senza la segnalazione di violazione.

Nel caso le segnalazioni risultasse **improcedibile o inammissibile** si potrà procedere all'archiviazione garantendo la tracciabilità delle motivazioni di inammissibilità.
Durante la verifica preliminare si possono chiedere ulteriori elementi per approfondimenti.

5.7 Istruttoria e accertamento della segnalazione

Il gestore delle segnalazioni deve effettuare tutte le verifiche sui fatti segnalati, garantendo tempestività e obiettività, competenza e diligenza professionale.
Nel caso in cui le segnalazioni riguardassero il gestore delle segnalazioni il segnalante dovrà rivolgersi all' Amministratore Unico o al Presidente del CDA.
L'attività di istruttoria e di accertamento è interamente a carico del gestore delle segnalazioni.
L'obiettivo della fase di accertamento e di procedere con le verifiche, le analisi e le valutazioni specifiche circa la fondatezza o meno dei fatti segnalati:

- acquisendo direttamente gli elementi informativi necessari alle valutazioni tramite l'analisi della documentazione e delle informazioni ricevute;
- se del caso coinvolgendo altre strutture aziendali o specialisti esterni,
- audizione di eventuali soggetti interni e/o esterni.

Nel caso si debba avvalersi dell'assistenza di professionisti terzi, coinvolgimento di altre persone interne e/o esterne, si oscurerà ogni tipologia di dato che possa consentire l'identificazione del segnalante e di ogni altra persona coinvolta (facilitatore, ulteriori persone menzionate).
In caso di segnalazioni di violazioni riguardanti il Modello 231 si opererà con l'ODV (se non nominato gestore delle segnalazioni)
Una volta completata l'attività di accertamento il gestore può:

- Archiviare la segnalazione perché considerata infondata, motivandone le ragioni;
- Dichiarare fondata la segnalazione e rivolgersi agli organismi interni competenti (Amministratore Unico/Presidente del CDA, Ufficio legale)**.**

Tutte le fasi dell'attività saranno sempre tracciate e archiviate correttamente.

5.8 Riscontro al segnalante

Il gestore deve dare un riscontro al segnalante entro tre mesi dalla data di avviso del ricevimento, o in mancanza di tale avviso entro tre mesi della data di scadenza del termine di sette giorni.

Se l'attività di accertamento non sarà conclusa entro tre mesi, considerando che vi sono delle fattispecie che richiedono verifiche in tempi maggiori, pertanto si tratta di un riscontro che può essere definito di natura interlocutoria se non definito.
Alla scadenza dei tre mesi il gestore può comunicare al segnalante:

- L'avvenuta archiviazione della segnalazione motivandone le ragioni;
- L'avvenuto accertamento della fondatezza della segnalazione e la sua trasmissione agli organi interni competenti;
- L'attività svolta fina a questo momento e/o l'attività che intende svolgere.

Nell'ultimo caso si comunicherà al segnalante anche il successivo esito finale dell'istruttoria.

6. LA TUTELA DEL SEGNALANTE E DEI SOGGETTI AD ESSO ASSIMILATI

Uno dei principali cardini della disciplina del whistleblowing è rappresentato dalle tutele riconosciute al segnalante per le segnalazioni effettuate per il rispetto della disciplina:

- l'obbligo di riservatezza della sua identità;
- il divieto di atti ritorsivi nei suoi confronti;
- la limitazione della sua responsabilità per la rilevazione e diffusione di alcune tipologie di informazioni protette.

Tali misure di protezione con alcune eccezioni si applicano anche ai soggetti, che potrebbero essere oggetto di ritorsioni, in ragione del loro ruolo assunto e della vicinanza o rapporto con il segnalante.
In particolare, si tratta dei seguenti soggetti:

- **Il facilitatore**, persona che assiste il segnalante nella segnalazione operante nel medesimo contesto lavorativo. Potrebbe essere un collega o un collega sindacalista che assiste il segnalatore a suo nome che però non può spendere la sigla sindacale. Se assiste il segnalante utilizzando la sigla sindacale lo stesso non riveste il ruolo di facilitatore;
- **persone nel medesimo contesto lavorativo del segnalante legato al segnalante da uno stabile legame affettivo e di parentela entro il quarto grado** (ad esempio famigliare o convivente) in modo di estendere il più possibile la tutela;
- **colleghi di lavoro** del segnalante che al momento lavorano nel medesimo contesto lavorativo;
- **enti di proprietà** anche in compartecipazione;
- **enti presso i quali il segnalante lavora.**

6.1 La riservatezza dell'identità del segnalante

Il Decreto prevede l'obbligo nei confronti del segnalante di garantire la riservatezza della sua identità, delle informazioni fornite e della relativa documentazione dalla quale si possa risalire alla sua identità.
A tale obbligo sono tenuti:

- i soggetti che ricevono e gestiscono la segnalazione;
- l'ANAC;
- le autorità amministrative cui l'ANAC trasmette per competenza le segnalazioni.

6.2 Il divieto e la protezione contro le ritorsioni

Il Decreto vieta ogni forma di ritorsione nei confronti del segnalante, ai facilitatori e altri soggetti, intesa come qualsiasi comportamento, atto od omissione, anche tentata, o minacciata, che si verifichi nel contesto lavorativo e che determini un danno, diretto o indiretto, ai soggetti tutelati.
Gli atti adottati in violazione del divieto sono nulli.
L'ANAC è l'ente preposto a ricevere dal segnalante le presunte ritorsioni subite e dovrà eseguire accertamenti e adottare i conseguenti provvedimenti.

Affinchè venga riconosciuta tale forma di tutela devono esserci le seguenti condizioni:

- che il segnalante al momento della segnalazione/denuncia avesse **fondati motivi** di ritenere le informazioni veritiere e rientranti nella disciplina;
- che la segnalazione/denuncia sia stata effettuata secondo la disciplina prevista da Decreto.

Questo implica da parte del segnalante un'attenzione nella valutazione delle informazioni che non possono fondarsi su supposizioni "voci di corridoio" o notizie di pubblico dominio.
La norma elenca le possibili ritorsioni anche se non esaustive:

- il licenziamento, la sospensione o misura equivalente;
- la retrocessione di grado o la mancata promozione, il mutamento di funzione, il cambio del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione o la restrizione della formazione;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di sanzioni anche pecuniarie;
- la coercizione, l'intimidazione, le molestie, l'ostracismo;
- la discriminazione o il trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine a tempo indeterminato, laddove il lavoratore ne avesse la legittima aspettativa;
- 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 pregiudizi economici o finanziari;
- l'inserimento di elenchi impropri, che dia l'impossibilità alla persona di trovare occupazione;
- la conclusione anticipata o l'annullamento di un contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoporsi ad accertamenti psichiatrici o medici.

Il soggetto che ritiene di aver subito una ritorsione, anche tentata o minacciata lo comunica all'ANAC, che accerterà il nesso tra la ritorsione e la segnalazione e adotterà le sanzioni. Se l'ANAC considerasse inammissibile la comunicazione l'archivierà.
Sarà il soggetto che si presuppone abbia effettuato la presunta ritorsione a dover dimostrarne la non veridicità o il procedimento disciplinare non è attinente alla segnalazione.
Nel caso di ritorsioni commesse nel contesto lavorativo di un soggetto del settore privato, l'Ufficio preposto informa l'Ispettorato Nazionale del Lavoro per i provvedimenti di competenza.
Infine, si specifica che il segnalante perde la protezione, quando viene accertato, con sentenza di primo grado, la responsabilità penale del segnalante per i reati di diffamazione, calunnia.

6.3 La limitazione di responsabilità del segnalante

Ulteriore tutela è la limitazione per il segnalante della sua responsabilità rispetto alla segnalazione di alcune categorie di informazioni, che altrimenti lo esporrebbero a responsabilità penali, civile amministrative. Il segnalante non sarà chiamato a rispondere:

- di rivelazione e utilizzazione del segreto d'uffici;
- di rivelazione del segreto professionale;
- di rivelazioni di segreti scientifici o industriali;
- di violazione del dovere di fedeltà e lealtà;
- di violazione delle disposizioni relative alla tutela del diritto d'autore;
- di violazione delle disposizioni relative alla protezione dei dati personali;

- di rivelazione o diffusione di informazioni sulle violazioni che offendono la reputazione della persona coinvolta.

Non è esclusa la responsabilità per condotte che:

- non siano collegate alla segnalazione;
- non siano strettamente necessarie a rivelare la violazione;
- l'acquisizione delle informazioni o l'accesso ai documenti sia effettuato in modo illecito.

7. TRATTAMENTO DEI DATI PERSONALI

Nel canale di segnalazione interna la società ha posto particolare attenzione al rispetto della disciplina della protezione dei dati personali (Regolamento UE n. 679/2016 e 196/2003 c.d. Codice privacy).

7.1 Il ricevimento e la gestione di una segnalazione

Il ricevimento e la ricezione di una segnalazione attivano per l'ente un trattamento dei dati personali:

- di natura comune, di natura particolare (ex dati sensibili) e giudiziari come condanne contenute nella segnalazione e negli atti;
- relative a tutte le persone fisiche identificate o identificabili e a vario titolo coinvolte;
- necessario per dare attuazione agli obblighi di legge previsti dalla disciplina whistleblowing la cui osservanza è condizione di liceità del trattamento (vedi Parere del Garante privacy);
- realizzato al solo fine di gestire e dare seguito alle segnalazioni (art.12, co.1 del Decreto);
- che, in ragione della particolare delicatezza delle informazioni potenzialmente trattate, della vulnerabilità degli interessati nel contesto lavorativo, nonché dello specifico regime di riservatezza dell'identità del segnalante previsto dal Decreto, presenta rischi specifici per i diritti e le libertà degli interessati (v. Parere del Garante privacy) e, pertanto, deve essere preceduto da una valutazione d'impatto sulla protezione dei dati, c.d. DPIA (art. 13, co. 6 del Decreto e artt. 35 e 36 del GDPR);
- rispetto al quale, l'esercizio dei diritti degli interessati (es. accesso, rettifica, aggiornamento, cancellazione, limitazione del trattamento, portabilità, opposizione) può essere limitato qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante (art. 13, co. 3 del Decreto e art. 2-undecies del Codice privacy).

7.2 Impostazione ed esecuzione dei trattamenti conseguenti alle segnalazioni

Ai fini della impostazione dei canali di segnalazione interna, il Decreto, oltre a rinviare al GDPR, ai relativi principi e al Codice privacy, detta specifiche garanzie per i trattamenti conseguenti alle segnalazioni.

In particolare, il Decreto dà specifica attuazione ai principi di:

- **trasparenza** (art. 5, par. 1, lett. a) del GDPR: i dati personali sono trattati in modo trasparente nei confronti dell'interessato);
- **limitazione delle finalità** (art. 5, par. 1, lett. b) del GDPR: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità), prevedendo che le segnalazioni non possano essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse (art. 12, co. 1 del Decreto);
- **minimizzazione dei dati** (art. 5, par. 1, lett. c) del GDPR: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

- **limitazione della conservazione** (art. 5, par. 1, lett. e) del GDPR: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

- **integrità e riservatezza** (art. 5, par. 1, lett. f) del GDPR: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali), prevedendo che l'individuazione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi del trattamento e promuovendo il ricorso a strumenti di crittografia (art. 4, co. 1 e art. 13, co. 6 del Decreto);

  Per definire i modelli di ricevimento e gestione delle segnalazioni, rilevano, altresì, i principi di:
  privacy by design e privacy by default (art. 25 del GDPR), che impongono di considerare le garanzie di protezione dei dati personali sin dalla progettazione del canale di segnalazione (privacy by design) e di assicurare che per impostazione predefinita (privacy by default) siano trattati solo i dati personali strettamente necessari in relazione alla specifica segnalazione e che tali dati non siano resi accessibili, in via automatica, a un numero indefinito di soggetti;
- **riservatezza**, su cui si basa l'intera disciplina whistleblowing. A tal fine, le LLGG prescrivono di garantire il divieto di tracciamento dei canali di segnalazione. Nel caso in cui l'accesso ai canali interni e al canale esterno di segnalazione avvenga dalla rete dati interna dell'ente e sia mediato da dispositivi firewall o proxy, deve essere garantita la non tracciabilità - sia sulla piattaforma informatica che negli apparati di rete eventualmente coinvolti nella trasmissione o monitoraggio delle comunicazioni - del segnalante nel momento in cui viene stabilita la connessione a tali canali.

Come altri trattamenti dei dati personali, anche quello del ricevimento e alla gestione delle segnalazioni deve essere censito nel **registro delle attività di trattamento** in conformità all'art. 38 del GDPR.

- Gli enti che attivano il canale interno effettueranno i trattamenti dei dati relativi al ricevimento e alla gestione delle segnalazioni in qualità di **Titolare del trattamento;**
- In caso di condivisione di risorse per la gestione gli enti tratteranno i dati come contitolari;
- In caso di affidamento del canale di segnalazione ad un esterno quest'ultimo dovrà trattare i dati in qualità di Responsabile esterno. (Con incarico scritto)

Le persone fisiche preposte alla ricezione e alla gestione delle segnalazioni tratteranno i dati in qualità di soggetti autorizzati al trattamento. (con incarico scritto)
i titolari del trattamento daranno ex ante, un'informativa, che non deve essere fornita a soggetti diversi dal segnalante, per evitare la possibilità di dedurre il coinvolgimento della persona e vanificarne le tutele.
I dati devono essere conservati cinque anni dalla comunicazione dell'esito finale della procedura.

8. SISTEMA SANZIONATORIO

Nell'ipotesi della mancata istituzione del canale, di mancante adozione delle procedure o di adozione procedure non conformi il responsabile è individuato nell'ente.
Nell'ipotesi in cui non sia stata svolta l'attività di verifica e analisi delle segnalazioni o violato l'obbligo di riservatezza il responsabile è il gestore delle segnalazioni.
Nell'ipotesi di sanzioni nei confronti di chi abbia adottato un atto ritorsivo, viene sanzionata la persona fisica individuata come responsabile delle ritorsioni.

Le sanzioni amministrative pecuniarie hanno un minimo di € 10.000 ad un massimo di 50.000 quando la persona fisica abbia commesso ritorsioni, abbia ostacolato o tentato di ostacolare la segnalazione, abbia violato l'obbligo di riservatezza, quando non sono stati istituiti canali di segnalazione, quando non sono state adottate procedure per la segnalazione delle violazioni o esse non siano conformi.

9. DISCIPLINA WHISTLEBLOWING E MODELLO ORGANIZZATIVO

Sarà necessario aggiornare il Modello Organizzativo con l'indicazione dei canali di segnalazione adottati dall'ente, avendo cura di esplicitare il divieto di commissioni di ritorsioni e il rispetto dei doveri di riservatezza.
Verrà altresì integrato il Sistema disciplinare del Modello considerato che la normativa richiede che venga adeguato prevedendo sanzioni nei confronti dei responsabili delle violazioni.
Si integrerà il Sistema Disciplinare per quanto riguarda la commissione di ritorsioni, alla non istituzione dei canali di segnalazione, sugli ostacoli delle segnalazioni e la violazione dell'obbligo di riservatezza.

10. ATTIVITÀ DI FORMAZIONE E INFORMAZIONE

Il Decreto al fine di garantire una gestione professionale delle segnalazioni mira a sensibilizzare i vari soggetti circa le implicazioni etiche, legali e di riservatezza che scaturiscono dalle segnalazioni.
L'art. 4 co. 2 prevede che gli uffici o le persone a cui è demandata la gestione del canale di segnalazione debbano ricevere una specifica formazione relativa alla gestione del canale.
L'art. 5 co. 1 lett. a prevede che gli uffici e le persone a cui è demandata la gestione del canale di segnalazione mettano a disposizione dei segnalanti informazioni chiare, sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni.
Tale formazione dovrà essere erogata con cadenza periodica.

11. SEGNALAZIONE ESTERNA E DIVULGAZIONE PUBBLICA

L'artico 7 del decreto attribuisce all'ANAC il compito di istituire un canale di segnalazione a tutti i soggetti con le medesime protezioni. (https://whistleblowing.anticorruzione.it)

11.1 Le condizioni per la segnalazione esterna

Per poter ricorrere al canale di segnalazione ANAC devono esserci le seguenti condizioni:

- nel contesto lavorativo non è stato previsto il canale interno o non attivato (come da obbligatorietà);
- la segnalazione interna non ha avuto seguito;
- ci sono fondati motivi di non seguito alla segnalazione o timore di ritorsioni;
- ci sono fondati motivi che la violazione possa essere un pericolo imminente o palese per il pubblico interesse.

In riferimento alle modalità di segnalazione esse possono essere effettuate:

- tramite piattaforma informatica come canale prioritario in quanto garantisce la massima riservatezza e protezione per il segnalante;
- oralmente, tramite un servizio telefonico con operatore che inserisce le comunicazioni nella piattaforma;
- tramite incontri diretti. (con richiesta motivata)

Per essere ammissibile il segnalante deve indicare: i suoi dati e il recapito, i fatti oggetto della segnalazione, l'ente ove sono avvenuti i fatti e il profilo professionale che riveste.
La segnalazione è inammissibile:

- per manifesta infondatezza per mancanza di elementi riconducibili alle violazioni enunciate;

- per manifesta insussistenza dei presupposti di legge per l'esercizio dei poteri di vigilanza dell'Autorità;
- per manifesta incompetenza dell'Autorità sulle questioni segnalate;
- per accertato contenuto generico della segnalazione, tale da non consentire la comprensione dei fatti;
- per produzione della sola documentazione in assenza della segnalazione esterna;
- per mancanza di dati che costituiscono elementi essenziali della segnalazione esterna;
- per sussistenza di segnalazione di lieve entità.

11.2 La procedura della divulgazione pubblica

Si tratta di una novità estremamente delicata per l'impresa, per le potenzialità lesive dell'ente di una denuncia effettuata in assenza di giustificati motivi e di prove fondate.
La divulgazione può essere effettuata tramite stampa ma anche tramite i social network e i canali come Facebook, Twitter ecc.
Si vuol far notare l'extrema ratio di tale divulgazione.
Prima di ricorrere a tale procedura deve ricorrere almeno una delle seguenti condizioni:

- che sia prima utilizzato il canale interno o esterno senza riscontro o non vi sia stato dato seguito entro i termini previsti dal Decreto;
- che il segnalante ritenga sussistere fondati motivi per un pericolo imminente per il pubblico interesse, considerato come situazione di emergenza o di rischio di danno irreversibile, anche all'incolumità fisica di una o più persone, che richieda che la violazione sia tempestivamente svelata con ampia risonanza per impedirne gli effetti;
- che per il segnalante vi siano fondati motivi che una segnalazione esterna comporti un rischio di ritorsione, oppure non avere efficace seguito perché potrebbe ricorrere un pericolo di distruzione delle prove o di collusione tra l'autorità preposta a ricevere la segnalazione. Dovrebbe in altri termini trattarsi di situazioni particolarmente gravi di negligenza o comportamenti dolosi all'interno dell'ente.

La Ditta

TAO AMBIENTE SRL

TAO AMBIENTE SRL