Manuale sul Whistleblowing e Protezione dei Whistleblower

Sommario

Riferimenti Normativi

Il whistleblowing è stato introdotto in Italia con una legislazione specifica a fine 2017 con la Legge n. 179. Questa normativa regolamentava in modo completo l'istituto per la pubblica amministrazione mentre introduceva alcune disposizioni anche per le organizzazioni del settore privato dotate di un modello organizzativo di gestione e controllo ex. D.lgs. n. 231/2001 (responsabilità degli enti). La Legge n. 179/2017 è stata successivamente superata dalla legge di trasposizione della Direttiva Europea in materia di whistleblowing (n. 1937/2019). Il nuovo documento, riconosce alla segnalazione un ruolo chiave nella prevenzione delle violazioni normative e assicura ai segnalanti di imprese sia pubbliche che private, una tutela più strutturata. Il decreto aggiorna così la legislazione italiana, armonizzandola con quelle che sono le norme del Parlamento europeo e del Consiglio circa la protezione delle persone che segnalano violazioni del Diritto dell'Unione e di disposizioni normative nazionali. Con il D. LGS 24/203 aumentano infatti le condotte meritevoli di segnalazione; la disciplina prevista dal decreto si estende infatti anche alle violazioni che possano ledere gli interessi dell'Unione Europea. Ricadono nella normativa anche le violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità della Pubblica Amministrazione o dell'ente privato, inclusi gli illeciti amministrativi, contabili, civili o penali. In continuità con il passato, vengono annoverate anche "le condotte illecite rilevanti ai sensi del Decreto legislativo 8 giugno 2001, n. 231 o violazioni dei modelli di organizzazione e di gestione". La nuova normativa prevede oneri in capo alle organizzazioni pubbliche e private, in particolare: tutti gli enti pubblici devono prevedere procedure interne per la gestione delle segnalazioni; lo stesso obbligo è in carico ai soggetti del settore privato che hanno un modello organizzativo ex D.lgs. n. 231/2001 e a tutte le organizzazioni private con almeno 50 dipendenti.

Scopo del Manuale

Le procedure di whistleblowing incoraggiano a segnalare chiunque acquisisca, nel contesto dell'attività lavorativa, informazioni sugli illeciti commessi dall'organizzazione o per conto dell'organizzazione. Il manuale sul whistleblowing è stato creato per promuovere la trasparenza, l'integrità e l'etica all'interno dell'organizzazione privata. Questo strumento è essenziale per garantire che i dipendenti e altri stakeholder abbiano un mezzo sicuro e confidenziale per segnalare comportamenti illeciti o non etici di cui vengono a conoscenza nell'ambito delle loro attività lavorative. La creazione di un ambiente di lavoro in cui tutti si sentano sicuri nel segnalare irregolarità è fondamentale per prevenire frodi, corruzione, molestie e altre violazioni delle normative aziendali e legali.

Pubblico di Destinazione

Il manuale è rivolto a:

- **Dipendenti e Collaboratori**: Tutti i dipendenti dell'organizzazione, indipendentemente dal loro livello gerarchico o posizione, sono incoraggiati a utilizzare le procedure di segnalazione per riportare qualsiasi comportamento sospetto o illecito. Questo gruppo include tutti i lavoratori con contratto a tempo indeterminato, determinato, part-time e full-time.
- **Collaboratori Esterni**: Include consulenti, fornitori e altri collaboratori esterni che, nello svolgimento delle loro attività, potrebbero venire a conoscenza di violazioni delle norme etiche o legali dell'organizzazione.
- **Manager e Dirigenti**: Hanno la responsabilità di promuovere e supportare l'uso del sistema di whistleblowing, garantendo che le segnalazioni siano gestite in modo equo e confidenziale.
- **Amministratori e Membri del Consiglio di Amministrazione**: Devono essere consapevoli delle politiche di whistleblowing e supportarne l'implementazione e l'aderenza.
- **Soggetti Coinvolti nei Processi di Governance e Controllo**: Questo gruppo include i membri dei comitati di controllo interno, i responsabili della compliance e gli auditor interni ed esterni.

Comportamenti e Violazioni da Segnalare

Nel contesto di un sistema di whistleblowing, è fondamentale specificare chiaramente quali tipi di comportamenti e violazioni devono essere segnalati dai dipendenti e dai collaboratori. Ecco una lista dettagliata delle principali categorie di illeciti che devono essere riportate:

- **Frodi**: Attività fraudolente volte a ottenere benefici finanziari illeciti.
- **Corruzione**: Atti di corruzione sia attiva che passiva.
- **Molestie e Discriminazioni**: Comportamenti che costituiscono molestie sessuali o morali, discriminazioni basate su razza, genere, orientamento sessuale, religione, età, disabilità o qualsiasi altra caratteristica protetta.
- **Violazioni della Sicurezza sul Lavoro**: Situazioni che mettono in pericolo la salute e la sicurezza dei lavoratori.
- **Irregolarità Amministrative**: Azioni che violano le politiche e le procedure aziendali.
- **Abuso di Ufficio**: Utilizzo improprio della posizione di potere.
- **Conflitti di Interesse**: Situazioni in cui gli interessi personali di un dipendente possono interferire con la capacità di svolgere i propri compiti in modo imparziale.
- **Violazioni di Leggi e Regolamenti**: Qualsiasi comportamento che costituisce una violazione delle leggi locali, nazionali o internazionali.
- **Parità di Genere**: Comportamenti che violano i principi di equità e parità di trattamento tra i sessi.

Canali di Segnalazione

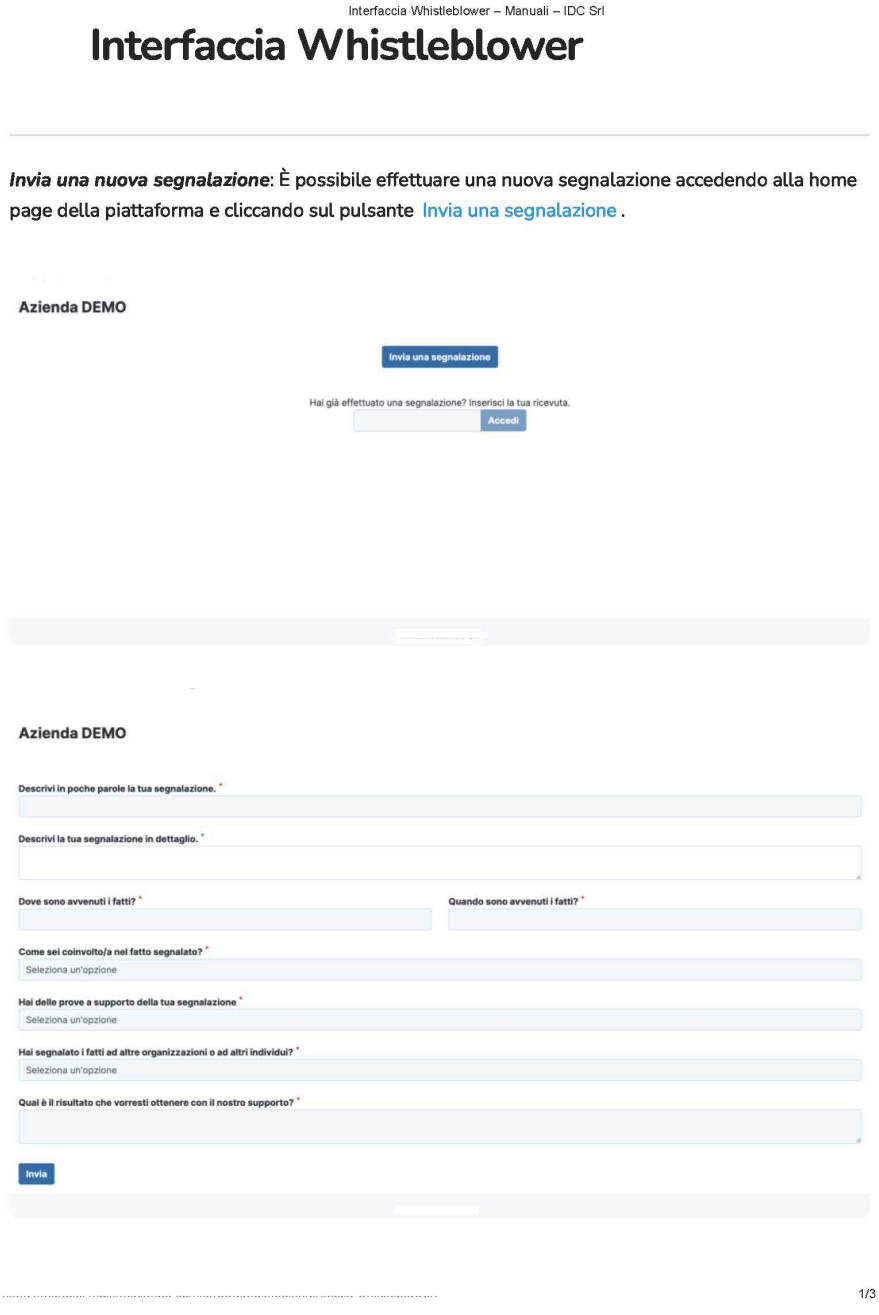
Il Responsabile per la Prevenzione della Corruzione e la Trasparenza (RPCT) è l'autorità designata per la ricezione e la gestione delle segnalazioni di illecito. Il RPCT può essere assistito da membri del suo gruppo di supporto, specificamente nominati attraverso atti interni. Il responsabile del whistleblowing, o l'ufficio preposto se nominato, riceve le segnalazioni e interagisce con il segnalante per chiarire e approfondire le informazioni ricevute. Questo dialogo continua anche durante le fasi di verifica. Dopo una valutazione preliminare, il responsabile o l'ufficio incaricato conduce un'accurata indagine delle informazioni segnalate, richiedendo eventualmente ulteriori dati ad altri uffici e funzioni dell'organizzazione. Il ricevente fornisce riscontri periodici al segnalante e, al termine dell'indagine, comunica i risultati. Nella comunicazione dell'esito non sono inclusi riferimenti a dati personali dell'eventuale soggetto segnalato. I possibili esiti comunicabili al segnalante includono:

- Correzione di processi interni
- Avvio di un procedimento disciplinare
- Trasferimento dei risultati dell'indagine alla procura della Repubblica e/o alla Corte dei conti in caso di danno erariale
- Archiviazione per mancanza di evidenze

Le segnalazioni erroneamente inviate al superiore gerarchico potrebbero non essere trattate come segnalazioni di whistleblowing, in quanto il superiore gerarchico non è vincolato agli stessi obblighi di riservatezza previsti per il soggetto ricevente.

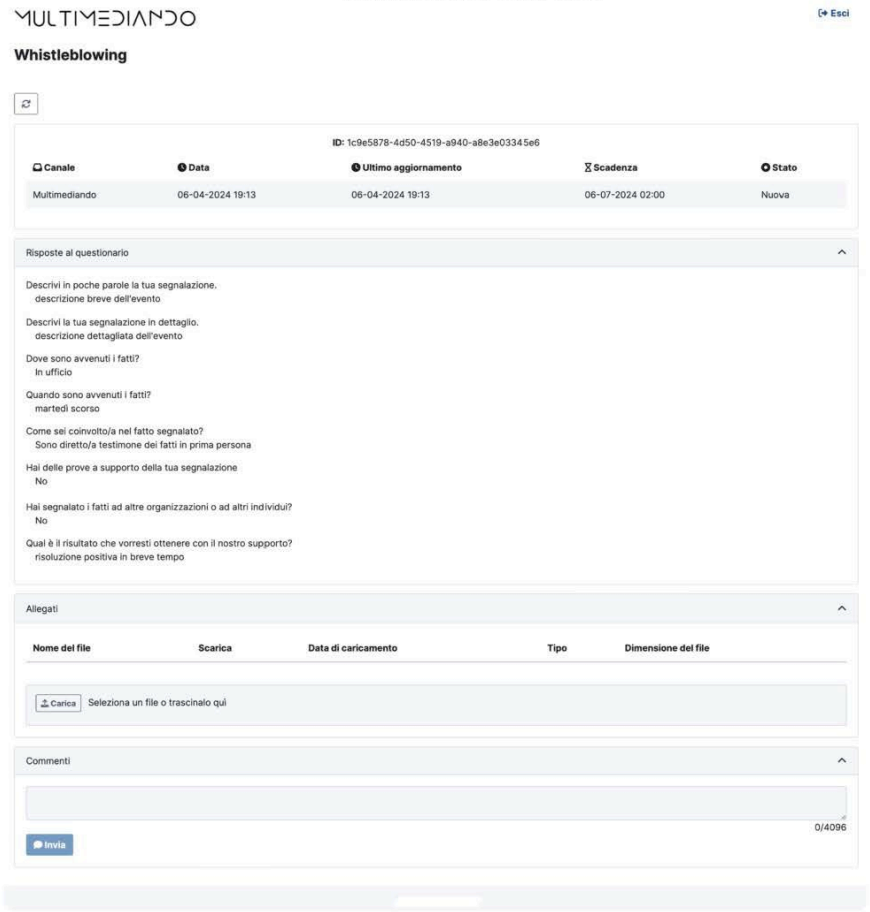
Canali disponibili per effettuare le segnalazioni:

I dipendenti possono accedere al sistema anonimo online attraverso il seguente link, disponibile anche sul portale interno dell'azienda: https://whisperguard.it/t/6c6baf15-9e2c-4cce-9ccb-17d104659848/#/



Dopo aver inviato la segnalazione il sistema fornisce all'utente una ricevuta di 16 cifre.

Accedere a una segnalazione esistente: È possibile accedere ad una segnalazione esistente inserendo la ricevuta di 16 cifre ottenuta al termine dell'invio sull'interfaccia di login presente nella home page della piattaforma.



3/3

Processo di Investigazione delle Segnalazioni di Whistleblowing

- **Ricezione delle Segnalazioni**
    - **Registrazione**: Quando una segnalazione viene ricevuta attraverso uno dei canali designati (email, telefono, sistema anonimo online), viene immediatamente registrata nel sistema di gestione delle segnalazioni dell'azienda.
    - **Conferma di Ricezione**: Una conferma della ricezione della segnalazione viene inviata al segnalante se non è anonima entro 7 giorni dalla ricezione.
- **Processo di Investigazione**

- **Prima Valutazione**: Un comitato interno effettua una valutazione preliminare della segnalazione per determinarne la credibilità e la rilevanza. La valutazione preliminare deve essere completata entro 15 giorni dalla ricezione della segnalazione.
- **Avvio dell'Investigazione**: Se la segnalazione viene ritenuta valida, viene nominato un investigatore o un team di investigazione. Questo può includere personale interno qualificato o, in casi complessi, investigatori esterni indipendenti.
- **Conduzione dell'Investigazione**: L'investigatore raccoglie tutte le prove pertinenti, conduce interviste confidenziali e analizza i dati raccolti.
- **Conclusione dell'Investigazione**: Al termine dell'investigazione, l'investigatore redige un rapporto finale che include un riassunto delle prove raccolte, le conclusioni tratte e le raccomandazioni per le azioni successive.

- **Responsabilità e Comunicazione**
  - **Comunicazione dei Risultati**: Il segnalante viene informato dell'esito dell'investigazione e delle eventuali azioni correttive prese.
  - **Azioni Correttive**: Il management è responsabile dell'implementazione delle azioni correttive raccomandate.
- **Monitoraggio**
  - **Follow-Up**: Viene effettuato un follow-up per garantire che le azioni correttive siano state implementate efficacemente e che non si verifichino ritorsioni contro il segnalante.

Protezione contro le Ritorsioni

Tutte le informazioni raccolte nel corso delle indagini sono trattate nel rispetto delle normative vigenti sulla protezione dei dati personali, garantendo che i dati siano conservati in modo sicuro e solo per il tempo strettamente necessario.

- **Riservatezza e Anonimato**: Il soggetto ricevente è tenuto a trattare le segnalazioni preservandone la riservatezza. Le informazioni relative all'identità del soggetto segnalante, del soggetto segnalato e di ogni altra persona menzionata nella segnalazione sono trattate secondo i principi di confidenzialità. L'identità della persona segnalante non può essere rivelata senza il suo consenso.
- **Segnalazioni Anonime**: È possibile anche l'invio di segnalazioni anonime. Il soggetto ricevente può decidere se processarle o meno, ma queste vengono trattate secondo gli stessi principi di riservatezza.
- **Protezione dei Dati Personali**: Le segnalazioni ricevute, le attività di accertamento e le comunicazioni tra la persona segnalante e la persona ricevente sono documentate e conservate in conformità alle prescrizioni in materia di riservatezza e protezione dei dati. Le segnalazioni possono essere trattate e mantenute solo per il tempo necessario al loro trattamento, e in nessun caso oltre i 5 anni successivi alla comunicazione dell'esito delle attività di accertamento.
- **Minimizzazione e Anonimizzazione**: Nel corso delle attività di accertamento, il soggetto ricevente può condividere con altre funzioni dell'ente informazioni preventivamente anonimizzate e minimizzate.

Conseguenze per le Violazioni della Politica Aziendale e del Whistleblowing

L'azienda adotta una politica di tolleranza zero nei confronti di qualsiasi comportamento illecito e nei confronti delle ritorsioni contro i segnalatori che agiscono in buona fede. Di seguito sono dettagliate le conseguenze per coloro che violano la politica aziendale o che attuano ritorsioni:

- **Violazioni della Politica Aziendale**
    - **Comportamenti Illeciti**: Qualsiasi dipendente trovato colpevole di comportamenti illeciti sarà soggetto a misure disciplinari severe, che possono includere avvertimenti formali, sospensione, retrocessione o licenziamento.
    - **Segnalazioni False o Maliziose**: I dipendenti che effettuano segnalazioni false o maliziose saranno anch'essi soggetti a misure disciplinari.
- **Ritorsioni contro i Segnalatori**
    - **Protezioni Legali**: La normativa italiana vieta qualsiasi forma di ritorsione o discriminazione contro i segnalanti. Qualsiasi accusa di ritorsione sarà immediatamente investigata e i responsabili saranno soggetti a severe misure disciplinari.

Entità di Protezione

- **ANAC (Autorità Nazionale Anticorruzione)**: Monitora le segnalazioni di illeciti e garantisce la protezione dei whistleblower.
- **Ispettorato Nazionale del Lavoro**: Interviene per proteggere i diritti del lavoratore in caso di ritorsioni.

Sanzioni Amministrative Specifiche

Il Decreto Legislativo n. 24/2023 prevede sanzioni amministrative, irrogabili da parte dell'Autorità Nazionale Anticorruzione, in caso di violazione delle norme sul whistleblowing. Le sanzioni riguardano in modo specifico eventuali ritorsioni contro i soggetti segnalanti, violazioni dell'obbligo di riservatezza, il boicottaggio a un tentativo di segnalazione, la mancata presa in carico di una segnalazione o un'insufficiente attività istruttoria avviata in seguito alla stessa. Sono altresì sanzionabili gli abusi del sistema di segnalazione, con possibili sanzioni per colui che calunnia o diffama un altro soggetto a mezzo della procedura. L'amministrazione può procedere disciplinarmente contro i soggetti responsabili di queste condotte.

Documentazione delle Procedure

L'azienda deve mantenere una documentazione dettagliata delle procedure di segnalazione e delle misure adottate per proteggere i segnalanti. Questo include:

- **Registrazioni delle Segnalazioni Ricevute**: Dettagliate informazioni su ogni segnalazione ricevuta.
- **Investigazioni Condotte**: Documentazione delle indagini condotte in risposta alle segnalazioni.
- **Azioni Correttive Implementate**: Dettagli delle misure correttive adottate in seguito alle segnalazioni.

Importanza della Protezione contro le Ritorsioni

La protezione contro le ritorsioni è un aspetto cruciale del sistema di whistleblowing dell'azienda. Garantire che i segnalanti non subiscano ritorsioni non solo è un obbligo legale, ma anche un impegno etico verso la promozione di un ambiente di lavoro sicuro e trasparente. Implementando queste misure, l'azienda dimostra il suo impegno nel trattare seriamente le segnalazioni di illeciti e nel proteggere coloro che hanno il coraggio di denunciare comportamenti scorretti. Questo impegno si traduce in:

- **Fiducia dei Dipendenti**: Creazione di un ambiente in cui i dipendenti si sentono sicuri nel segnalare illeciti.
- **Miglioramento dell'Etica Aziendale**: Promozione di pratiche aziendali etiche e trasparenti.

- **Prevenzione delle Irregolarità**: Maggiore capacità di individuare e correggere le irregolarità prima che diventino problemi più gravi.

Sicurezza delle applicazioni Web

Questa sezione descrive la sicurezza delle applicazioni Web implementata dal software in conformità con le linee guida di sicurezza OWASP. Le misure di sicurezza adottate per proteggere le segnalazioni includono la crittografia avanzata dei dati in transito e in archiviazione, audit regolari dei nostri sistemi e formazione continua del personale sulla sicurezza delle informazioni.

- **Gestione della sessione**: L'implementazione della sessione segue le linee guida di sicurezza OWASP Session Management Cheat Sheet.

Il sistema genera una Sessione per ogni utente autenticato. L'ID sessione è crittografato, generato casualmente dal backend. Ogni sessione scade dopo un timeout di 60 minuti. Gli ID di sessione vengono scambiati dal client con il backend tramite un header (X-Session) e scadono non appena gli utenti chiudono il browser o la scheda su cui è in esecuzione la piattaforma. Gli utenti possono disconnettersi esplicitamente tramite un pulsante di disconnessione o chiudendo il browser.

- **Cookie e prevenzione XSRF***:* I cookie non vengono utilizzati intenzionalmente per ridurre al minimo gli attacchi XSRF e ogni possibile attacco basato su di essi. Invece di utilizzare i cookie, l'autenticazione si basa su un'intestazione di sessione HTTP personalizzata inviata dal client su richieste autenticate.
- **Intestazioni http**: Il sistema implementa un ampio set di intestazioni HTTP specificatamente configurate per migliorare la sicurezza del software e ottiene il punteggio A+ da Security Headers e il punteggio A+ da Mozilla Observatory.
- **Politica di sicurezza dei contenuti**: Il backend implementa una rigorosa politica di sicurezza dei contenuti (CSP) che impedisce qualsiasi interazione con risorse di terze parti e limita l'esecuzione di input di utenti non attendibili.