PROCEDURA WHISTLEBLOWING

SOMMARIO

1. AMBITO DI APPLICAZIONE

La presente Procedura Whistleblowing (di seguito "Procedura") si applica a Fondazione IEO-MONZINO ETS In particolare, i destinatari della presente procedura sono:

- i vertici aziendali ed i componenti degli organi sociali;
- i dipendenti e i collaboratori aziendali (a titolo di solo esempio: stagisti, tirocinanti, lavoratori somministrati etc.), anche in periodo di prova o cessati;
- i partner commerciali, i clienti, i fornitori, i consulenti, i soci e, più in generale, chiunque sia in relazione d'interessi con la società;

(d'ora in avanti collettivamente "Destinatari").

2. INFORMATIVA

La legge 179/2017, il D.Lgs. 231/2001 e il D.Lgs 24/2023, prevedono l'adozione di uno strumento informatico all'interno delle Organizzazioni Pubbliche e Private, attraverso il quale i dipendenti, collaboratori e tutti i soggetti identificati dalla normativa come possibili Whistleblower, 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.

L'obiettivo della direttiva europea è 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 di un'organizzazione, sia all'esterno. In casi specifici, è prevista la possibilità di effettuare la segnalazione mediante la divulgazione pubblica attraverso i media.

La nuova disciplina 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 pubblico o private.

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

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

3. PROCEDURA

Tutti i Destinatari della presente Procedura sono tenuti a segnalare potenziali attività illecite che possano violare la legge, il Codice Etico o le politiche di Fondazione IEO-MONZINO ETS. La segnalazione di possibili violazioni è incoraggiata, per consentire alla società di indagare nel merito e adottare le necessarie misure correttive. Dette misure consentono a Fondazione IEO-MONZINO ETS di ridurre eventuali rischi o danni per il singolo dipendente, i colleghi, la società stessa o le comunità in cui opera.

A tal fine, chiunque voglia effettuare una segnalazione può, a sua scelta e discrezione utilizzare il canale di comunicazione raggiungibile mediante collegamento al portale GRC CORA WHISTLEBLOWING, che consente di effettuare segnalazioni in forma anonima o nominativa.

Il segnalante può ovviamente utilizzare anche altri canali di segnalazione esterni purché ciò avvenga in conformità alla legge.

4. FORME DI TUTELA

Fondazione IEO-MONZINO ETS ha previsto l'incarico della gestione delle segnalazioni a figure responsabili appositamente designate. Tali figure in qualità di istruttori delle segnalazioni sono state adeguatamente autorizzate e nominate al trattamento dei dati personali e formate in tal senso.

Nel corso delle verifiche potranno essere coinvolti altri soggetti interni all'azienda per richiesta di informazioni o pareri ma rimarranno assolutamente estranei al dettaglio della segnalazione e a qualsiasi elemento che possa portare all'identificazione del soggetto segnalante.

Il portale permette di:

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

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

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

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

Sicurezza della piattaforma

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

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

- **Data Retention Policy**: Ogni segnalazione memorizzata nel Database incrementa l'attrattiva per potenziali Hacker. Le segnalazioni hanno una data di validità che può essere estesa dal *Receiver*, una segnalazione scaduta viene rimossa insieme a tutti i suoi dati
- **Server Resiliency**: Il Server è configurato in modo da rendere inoffensivi attacchi di tipo D/DOS. Richieste massive provenienti da uno stesso indirizzo IP che possano configurarsi come attacco, sono automaticamente inibite.
- **Web content security:** La comunicazione tra front end e back end utilizza le best practice, condivise a livello internazionale, tra cui header di sicurezza e cifratura della comunicazione con TLS 1.3.
- **File Encryption:** Un receiver può utilizzare la propria chiave PGP, se posseduta. Ciascun file è salvato su *dicker* utilizzando una chiave simmetrica casuale AES, la chiave è salvata su ramdisk
- **GDPR:** La Piattaforma di Whistleblowing è a norma con il regolamento generale sulla protezione dei dati (GDPR – General Data Protection Regulation, regolamento UE 2016/679)

5. COSA SEGNALARE

Le segnalazioni hanno ad oggetto fatti (di qualsivoglia natura, anche meramente omissivi), già accaduti o che molto verosimilmente potrebbero accadere, riferibili a Persone della società Fondazione IEO-MONZINO ETS o a Terzi che possano integrare illeciti, irregolarità o comunque condotte poste in essere in violazione:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del decreto legislativo 231/2001, o violazioni dei modelli di organizzazione e gestione ivi previsti;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- atti od omissioni che ledono gli interessi finanziari dell'Unione;
- atti od omissioni riguardanti il mercato interno;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.

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

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

Sono escluse le comunicazioni, doglianze, rivendicazioni, istanze aventi ad oggetto tematiche differenti da quelle delle segnalazioni. Le segnalazioni non devono riguardare rimostranze di carattere personale.

6. PERCHÉ DOVRESTI FARE UNA SEGNALAZIONE?

Le segnalazioni fatte in buona fede e nell'interesse del bene comune possono permettere di individuare per tempo e porre rimedio a comportamenti irregolari o illeciti che possono danneggiare la società.

7. VIOLAZIONE DELLA PRESENTE PROCEDURA E RESPONSABILITA' DEL SEGNALANTE

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

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

8. CONTENUTO DELLA SEGNALAZIONE

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

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

a) qualifica del soggetto che effettua la segnalazione;
b) descrizione dei fatti oggetto di segnalazione, con indicazione, se conosciute, delle circostanze di tempo e di luogo in cui sono stati commessi;
c) le generalità o altri elementi che consentano di identificare il soggetto/i che ha/hanno posto/i in essere i fatti segnalati;
d) l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
e) eventuali persone a conoscenza dei fatti;
f) allegare eventuali documenti o file multimediali utili ai fatti;
g) ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

9. TRASMISSIONE DELLA SEGNALAZIONE

Al fine di consentire al segnalante di procedere con la segnalazione in modo tempestivo, Fondazione IEO-MONZINO ETS ha messo a disposizione sul proprio sito web un apposito portale GRC CORA Whistleblowing raggiungibile al seguente indirizzo web fondazioneieomonzino.openblow.it**.** Dopo l'accesso al Portale il segnalante sarà guidato nella compilazione di un questionario formato da domande aperte e/o chiuse che gli permetteranno di fornire gli elementi caratterizzanti la segnalazione (fatti, contesto temporale, dimensioni economiche, etc.).

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

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

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

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

Tale KEY CODE non va assolutamente perso.

Inoltre si possono effettuare le segnalazioni attraverso i seguenti canali, anche se non preferenziali:

- chiamando il numero 02/669951, in questo caso la segnalazione viene verbalizzata per iscritto a cura dell'istruttore;
- incontro diretto con un istruttore, l'incontro verrà verbalizzato e sottoscritto.

10. GESTIONE DELLA SEGNALAZIONE

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

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

11. CONSERVAZIONE DELLA SEGNALAZIONE E PRIVACY

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