WHISTLEBLOWINGPA

PROCEDURA DI GESTIONE DELLE SEGNALAZIONI

Documento aggiornato al 03/04/2024 e condiviso con le organizzazioni sindacali comparativamente più rappresentative sul piano nazionale, delle rappresentanze sindacali aziendali di queste ultime ovvero della rappresentanza sindacale unitaria

APPROVATO CON DELIBERA DI CONSIGLIO N. 494 DEL 03/04/2024

Il presente documento è un modello di procedura di gestione delle segnalazioni ricevute e gestite tramite la piattaforma WhistleblowingPA e gli altri canali interni attivati per gestire le segnalazioni, che garantiscono, tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

La procedura adottata dall'ente dovrà essere revisionata annualmente, in concomitanza con la revisione del Piano Triennale di Prevenzione della Corruzione e in occasione di eventuali novità normative.

Sommario

1. Riferimenti normativi 1
2. Chi può effettuare una segnalazione 2
3. Cosa può essere segnalato..... **Errore. Il segnalibro non è definito.**
4. Chi riceve e gestisce le segnalazioni 3
5. I canali per le segnalazioni 4
6. Le tempistiche di gestione delle segnalazioni..... 5
7. Riservatezza e anonimato..... 5
8. La gestione dei dati personali 6
9. Tutele e protezioni 6
10. Sanzioni 7
11. Canali esterni per le segnalazioni ..... **Errore. Il segnalibro non è definito.**

1. 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.

La legge n.179/2017 è stata superata dalla legge di trasposizione della Direttiva Europea in materia di *whistleblowing* (n.1937/2019). La nuova legge, il Decreto Legislativo n.24/2023, è l'attuazione della Direttiva UE n.2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

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.

2. Chi può effettuare una segnalazione

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.

Lo scopo della procedura è quello di facilitare la comunicazione di informazioni relative a violazioni riscontrate durante l'attività lavorativa. A tale scopo lo spettro delle potenziali persone segnalanti è molto ampio. La procedura è volta a garantire questi soggetti, nel momento in cui segnalino una condotta illecita relativa all'ente.

Possono effettuare una segnalazione attraverso la procedura le seguenti categorie di soggetti:

- Dipendenti
- Collaboratori
- Fornitori, subfornitori e dipendenti e collaboratori degli stessi
- Liberi professionisti, consulenti, lavoratori autonomi
- Volontari e tirocinanti, retribuiti o non retribuiti
- Azionisti o persone con funzione di amministrazione, direzione, vigilanza, controllo o rappresentanza
- Ex dipendenti, ex collaboratori o persone che non ricoprono più una delle posizioni indicate in precedenza
- Soggetti in fase di selezione, di prova o il cui rapporto giuridico con l'ente non sia ancora iniziato

La procedura protegge anche l'identità dei soggetti facilitatori, le persone fisiche che assistono una persona segnalante nel processo di segnalazione, operanti all'interno del medesimo contesto lavorativo.

Non sono prese in considerazione, pertanto, le segnalazioni presentate da altri soggetti, ivi inclusi i rappresentanti di organizzazioni sindacali, in quanto l'istituto del *whistleblowing* è indirizzato alla tutela della singola persona fisica che agisce in proprio, non spendendo la sigla sindacale. In tale ultimo caso, le segnalazioni sono archiviate in quanto prive del requisito soggettivo previsto dalla normativa e, se relative a materie di competenza dell'ente, sono trattate quali segnalazioni ordinarie.

Si rammenta che la segnalazione e la documentazione ad essa allegata sono sottratte al diritto di accesso

agli atti amministrativi previsto dagli artt. 22 e seguenti della legge 241/1990, all'accesso civico generalizzato di cui all'art. 5 co. 2 del d.lgs. 33/2013 nonché all'accesso di cui all'art. 2-undecies co. 1 lett. f) del codice in materia di protezione dei dati personali

3. Cosa può essere segnalato

All'interno di questa procedura possono essere segnalati fatti illeciti di cui si sia venuti a conoscenza nel contesto della propria attività lavorativa. Possono essere riportati anche sospetti, qualificati, di reati o altre violazioni di disposizioni di legge o potenziali rischi di commissione degli stessi.

Non viene richiesto alla persona segnalante di dimostrare in modo completo la commissione di un illecito ma le segnalazioni devono essere quanto più possibile circostanziate, al fine di consentire un

accertamento dei fatti comunicati da parte dei soggetti riceventi. Allo stesso tempo, non si invitano i soggetti segnalanti ad attuare attività di investigazione che possano esporli individualmente.

Le segnalazioni possono riguardare illeciti penali, civili, amministrativi o contabili, così come le violazioni di normative comunitarie.

Non rientrano nell'oggetto di questa procedura le segnalazioni di carattere personale, per esempio inerenti al proprio contratto di lavoro, che sono regolate da altre procedure dell'ente.

4. Chi riceve e gestisce le segnalazioni

Il Responsabile per la Prevenzione della Corruzione e la Trasparenza (RPCT) è il soggetto responsabile alla ricezione e gestione delle segnalazioni di illecito, denominato "gestore" della segnalazione. Il RPCT può essere coadiuvato da soggetti del suo gruppo di supporto specificamente nominati in atto interno.

Il responsabile *whistleblowing*, o l'ufficio *whistleblowing* ove nominato, riceve le segnalazioni e dialoga con la persona segnalante per chiarire e approfondire quanto ricevuto. Il dialogo con la persona segnalante continua anche durante le fasi di accertamento.

Il responsabile o l'ufficio, dopo una valutazione iniziale, svolgono un'attività di accertamento delle informazioni segnalate, anche richiedendo specifiche informazioni ad altri uffici e funzioni interni all'organizzazione.

Il ricevente fornisce riscontri periodici alla persona segnalante e, al termine dell'attività di accertamento, comunica l'esito delle attività di accertamento. Nella comunicazione dell'esito non sono inclusi riferimenti a dati personali relativi all'eventuale soggetto segnalato.

Tra i possibili esiti che possono essere comunicati alla persona segnalante ci sono:

- Correzione di processi interni
- Avvio di un procedimento disciplinare
- Trasferimento dei risultati delle attività di accertamento alla procura della Repubblica (e/o della Corte dei conti in caso di danno erariale)
- Archiviazione per mancanza di evidenze

Si precisa che le segnalazioni devono specificare che si vuole mantenere riservata la propria identità e beneficiare delle tutele previste nel caso di eventuali ritorsioni per poter essere trattata come "segnalazione whistleblowing". Eventuali segnalazioni inviate ad un soggetto interno diverso dal gestore, qualora la segnalazione sia considerata "segnalazione whistleblowing", va trasmessa, entro sette giorni dal suo ricevimento, al soggetto interno competente (RPCT/Gestore), dandone contestuale notizia della trasmissione alla persona segnalante; in particolare, laddove il segnalante dichiari espressamente di voler beneficiare delle tutele in materia whistleblowing o tale volontà sia desumibile dalla segnalazione, la segnalazione è considerata "segnalazione whistleblowing" e va trasmessa, entro sette giorni dal suo ricevimento, al soggetto interno competente, dando contestuale notizia della trasmissione alla persona segnalante. Diversamente, se il segnalante non dichiari espressamente di voler beneficiare delle tutele, o detta volontà non sia desumile dalla segnalazione, detta segnalazione è considerata quale segnalazione ordinaria.

La segnalazione che venga erroneamente inviata al superiore gerarchico potrebbe non essere trattata come una segnalazione di *whistleblowing*, in quanto quest'ultimo non ha gli stessi obblighi di riservatezza in carico al soggetto ricevente; infatti, il d.P.R. n. 62 del 2013 prevede che la segnalazione possa essere presentata al superiore gerarchico: quest'ultimo, ove il segnalante dichiari di volersi avvalere delle tutele come whistleblower o tale volontà sia desumibile dalla segnalazione, è tenuto alla trasmissione al soggetto competente, entro sette giorni, come sopra indicato.

5. canali per le segnalazioni

L'ente mette a disposizione delle persone segnalanti canali diversi per le segnalazioni di violazioni ai sensi della presente procedura. In particolare, è possibile effettuare segnalazioni in forma orale e in forma scritta. Come confermato da ANAC, si ritiene che la posta elettronica ordinaria e la PEC siano strumenti non adeguati a garantire la riservatezza.

Per quanto riguarda le segnalazioni in forma scritta, l'ente mette a disposizione una piattaforma informatica crittografata, fornita da *Transparency International Italia* e *Whistleblowing Solutions* attraverso il progetto WhistleblowingIT. La piattaforma utilizza *GlobaLeaks*, il principale software open-source per il *whistleblowing*. Questo strumento garantisce, da un punto di vista tecnologico, la riservatezza della persona segnalante, dei soggetti menzionati nella segnalazione e del contenuto della stessa.

Il link di accesso alla piattaforma è pubblicato sul sito dell'ente in home page e in Amministrazione Trasparente | Altri Contenuti | Prevenzione della Corruzione.

Sulla piattaforma è caricato un questionario che guida la persona segnalante nel percorso di segnalazione attraverso domande aperte e chiuse, di cui alcune obbligatorie. È anche possibile allegare documenti alla segnalazione. Al termine della segnalazione la persona segnalante riceve un codice univoco di 16 cifre, con il quale può accedere alla segnalazione e dialogare in maniera bidirezionale con il soggetto ricevente, scambiare messaggi e inviare nuove informazioni. Tutte le informazioni contenute sulla piattaforma sono crittografate e possono essere lette solo da soggetti abilitati alla ricezione della segnalazione.

Per la gestione delle chiavi crittografiche si rinvia al documento allegato.

Non è possibile gestire altre segnalazioni ricevute in forma scritta. Qualora queste fossero inviate, il soggetto ricevente, ove possibile, inviterà la persona segnalante a presentare nuovamente la segnalazione tramite la piattaforma informatica.

Per le segnalazioni in forma orale, invitiamo la persona segnalante a contattare il soggetto ricevente, tramite i canali istituzionali, richiedendo disponibilità per un incontro personale con il RPCT, che verrà fissato entro massimo i 15 giorni successivi. Le segnalazioni in forma orale, previa presentazione dell'informativa del trattamento dei dati personali e delle indicazioni necessarie per reperire online il testo completo di tale informativa, vengono raccolte e verbalizzate dal RPCT e/o dal personale addetto specificamente autorizzato e il verbale deve essere firmato dalla persona segnalante, affinché sia processato. È opportuno ricordare che le segnalazioni in forma orale non offrono la stessa riservatezza tecnologica delle segnalazioni effettuate tramite piattaforma crittografata.

Il verbale della segnalazione resa in forma orale, la documentazione e gli atti acquisita anche a seguito dell'attività istruttoria del gestore, è conservata nei sistemi informatici dell'ente in partizioni il cui accesso è consentito solamente al personale autorizzato su volumi crittografati; i sistemi sono garantiti tramite backup incrementale che permetta una sufficiente storicità di recupero e al tempo stesso anch'esso su volumi crittografati e non accessibili a chi sprovvisto di autorizzazione.

Per i dati e documenti che necessitano di protocollazione, la stessa sarà riservata mediante autonomo registro accessibili solo al personale autorizzato.

In caso di passaggio dell'incarico da un RPCT all'altro, non appena l'RPCT lascia l'incarico, occorre modificare le credenziali di accesso al sistema.

L'ente garantisce, inoltre, il divieto di tracciamento dei canali di segnalazione, ovvero la non tracciabilità – sia sulla piattaforma informatica che negli apparati di rete eventualmente coinvolti nella trasmissione o monitoraggio delle comunicazioni - del segnalante, con particolare riguardo ai log generati (per esempio dagli apparati firewall) che possano contenere, tra gli altri, l'indirizzo IP della postazione di lavoro utilizzata per la connessione all'applicativo in questione e la username del soggetto ha effettuato tale connessione.

In particolare, è inibito il tracciamento degli accessi al sistema informatico deputato alla raccolta delle segnalazioni, in particolare quando questo è accessibile esclusivamente da postazioni di lavoro attestate alla rete aziendale interna (es. dispositivi quali firewall e web filtering sono in grado di memorizzare in appositi file di log le operazioni di navigazione effettuate, unitamente a dati che consentono di risalire anche indirettamente ai dipendenti o ad altri soggetti che le hanno effettuate).

6. Le tempistiche di gestione delle segnalazioni

Al termine del percorso di segnalazione la piattaforma mostra un codice di ricevuta a conferma che la segnalazione è stata consegnata e presa in carico dal soggetto ricevente.

Entro 7 giorni, il soggetto ricevente conferma alla persona segnalante la presa in carico della segnalazione e invita il soggetto segnalante a monitorare la sua segnalazione sulla piattaforma per rispondere a possibili richieste di chiarimenti o approfondimenti.

Entro 3 mesi dal giorno della segnalazione, il soggetto ricevente comunica alla persona segnalante un riscontro rispetto alle attività di accertamento svolte per verificare le informazioni comunicate nella segnalazione.

Il riscontro fornito entro 3 mesi può coincidere con l'esito delle attività di accertamento. Qualora queste non fossero concluse, il ricevente invita la persona segnalante a tenere monitorata la piattaforma fino a conoscere l'esito definitivo delle stesse.

L'avviso è rilasciato salvo il caso in cui l'ente ritenga che tale comunicazione potrebbe pregiudicare la tutela della riservatezza dell'identità della persona segnalante (si pensi, a tale riguardo, alle segnalazioni effettuate in forma orale).

7. 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. Allo stesso modo, sono trattate in modo confidenziale anche tutte le informazioni contenute nella segnalazione.

L'identità della persona segnalante non può essere rivelata senza il suo consenso. La conoscenza delle segnalazioni e dei relativi atti di accertamento sono sottratti anche al diritto all'accesso amministrativo da parte dei soggetti interessati.

L'unico motivo di possibile rivelazione dell'identità della persona segnalante può avvenire nel caso in cui gli atti di accertamento siano inoltrati presso una procura ordinaria o contabile e la conoscenza della stessa sia necessaria ai fini del diritto di difesa durante un procedimento giudiziario ordinario o contabile presso la Corte dei conti.

La riservatezza è garantita attraverso strumenti tecnologici, quali la piattaforma crittografata per le segnalazioni e un protocollo riservato, e all'interno di processi organizzativi volti a minimizzare la circolazione delle informazioni.

È possibile anche l'invio di segnalazioni anonime. Il soggetto ricevente può decidere se processarle o meno. In ogni caso, le segnalazioni vengono trattate secondo gli stessi principi di riservatezza. Tuttavia, nel caso di segnalazioni anonime, il soggetto ricevente non ha conoscenza dell'identità della persona segnalante e potrebbe involontariamente esporlo durante le attività di accertamento.

8. La gestione 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 contengono dati personali e possono essere trattate e mantenute solo per il tempo necessario al loro trattamento: questo tempo comprende l'analisi, le attività di accertamento e quelle di comunicazione degli esiti, oltre a una eventuale tempistica ulteriore per possibili commenti aggiuntivi. In nessun caso le segnalazioni saranno conservate oltre i 5 anni successivi alla comunicazione dell'esito delle attività di accertamento alla persona segnalante.

Per quanto riguarda l'accesso ai dati personali, questi sono conosciuti solo dal soggetto ricevente e, se indicato in specifico atto organizzativo, dai membri dello staff di supporto alla gestione della segnalazione.

Nel corso delle attività di accertamento il soggetto ricevente può condividere con altre funzioni dell'ente informazioni preventivamente anonimizzate e minimizzate rispetto alle specifiche attività di competenza di queste ultime.

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

Quanto alle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti in esame (artt. 24, 25 e 32 del Regolamento), in accordo con i consulenti tecnici dell'ente e in aggiunta al sistema di protezione già in uso, si avrà cura di:

- Adottare misure tecniche per il controllo degli accessi, che consentano di limitare l'accesso ai dati personali ai soli soggetti autorizzati dotati di credenziali di autenticazione e di uno specifico profilo di autorizzazione;
- Cifrare i dati personali sia in transito che *at rest* al fine di rendere incomprensibili i dati personali a chi non abbia un'apposita autorizzazione di accesso;
- Determinare tutto ciò che deve essere crittografato (incluso, in via non esaustiva, dischi rigidi, file, dati provenienti da un database o canali di comunicazione);
- Scegliere il tipo di crittografia in base al contesto e ai rischi individuati prediligendo soluzioni di crittografia basate su algoritmi pubblici notoriamente forti;
- Definire misure per garantire la disponibilità e l'integrità delle informazioni e ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- Determinare ciò che deve essere anonimizzato in base al contesto e alla forma in cui vengono memorizzati i dati personali (compresi i campi del database o estratti dai testi);
- Ridurre la possibilità che i dati personali possano essere correlati;
- Definire una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

9. Tutele e protezioni

La persona cui si fa riferimento nella segnalazione come responsabile del sospetto di illecito beneficia di misure di protezione dell'identità analoghe a quelle della persona segnalante e delle altre persone menzionate nella segnalazione.

In aggiunta alla tutela della riservatezza dell'identità della persona segnalante e dei soggetti menzionati nella segnalazione, nonché del contenuto della stessa, esistono altre forme di tutela garantite attraverso questa procedura.

Viene infatti garantita protezione alla persona segnalante contro ogni forma di ritorsione o discriminazione che dovesse subire in seguito e a causa di una segnalazione. Per ritorsione si intende qualsiasi azione o omissione minacciata o reale, diretta o indiretta, collegata o derivante da segnalazioni di illeciti effettivi o sospetti, che causi o possa causare danni fisici, psicologici, danni alla reputazione della persona, perdite economiche.

Tra le possibili discriminazioni rientrano:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- note di merito o referenze negative;
- misure disciplinari o altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o un trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto a termine;
- danni, anche alla reputazione della persona, pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e di redditi;
- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore in futuro;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; l'annullamento di una licenza o di un permesso; la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

10. Sanzioni

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.

11. Canali esterni per le segnalazioni

Al di fuori della procedura interna per le segnalazioni, la legge permette di effettuare anche segnalazioni esterne all'Autorità Nazionale Anticorruzione.

La persona segnalante può segnalare esternamente all'ente qualora abbia già effettuato una segnalazione a cui non è stato dato seguito, qualora abbia fondati motivi di ritenere che a una segnalazione interna non sia dato seguito o che questa possa determinare un rischio di ritorsione o qualora abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le modalità di segnalazione all'Autorità Nazionale Anticorruzione sono disponibili alla pagina dedicata sul sito dell'ANAC: anticorruzione.it/-/whistleblowing.

Esistono condizioni ulteriori per cui una persona segnalante possa effettuare una divulgazione pubblica: il mancato riscontro a una segnalazione interna o esterna previamente effettuata, un pericolo imminente o palese per l'interesse pubblico, fondati motivi che una segnalazione interna non verrà trattata o che le prove della stessa possano essere distrutte o occultate.