

WHISTLEBLOWING

MODELLO DI RICEVIMENTO E GESTIONE DELLE SEGNALAZIONI INTERNE



COMUNE DI ASIAGO

PREMESSA

Il D.Lgs. 10 marzo 2023, n. 24, ha recepito in Italia la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

Come previsto dall'art. 10 del D.Lgs. n. 24/2023, l'ANAC, con delibera n. 311 del 12 luglio 2023, ha approvato le "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne."

Le principali novità contenute nella nuova disciplina, rilevanti ai fini della redazione del presente modello, sono:

- la specificazione dell'ambito soggettivo con riferimento agli enti di diritto pubblico;
- l'ampliamento del novero delle persone fisiche che possono essere protette per le segnalazioni, denunce o divulgazioni pubbliche;
- l'espansione dell'ambito oggettivo, cioè di ciò che è considerato violazione rilevante ai fini della protezione, nonché distinzione tra ciò che è oggetto di protezione e ciò che non lo è;
- la disciplina di tre canali di segnalazione e delle condizioni per accedervi: interno, esterno (gestito da ANAC) nonché il canale della divulgazione pubblica;
- l'indicazione di diverse modalità di presentazione delle segnalazioni, in forma scritta o orale;
- la disciplina dettagliata degli obblighi di riservatezza e del trattamento dei dati personali ricevuti, gestiti e comunicati da terzi o a terzi;

- la disciplina sulla protezione delle persone segnalanti o che comunicano misure ritorsive offerta sia da ANAC che dall'autorità giudiziaria e maggiori indicazioni sulla responsabilità del segnalante e sulle scriminanti.

Il D.Lgs. 24/2023 prevede un sistema diversificato di presentazione delle segnalazioni:

1. Il canale interno dell'ente - incoraggiato
2. Il canale esterno presso ANAC
3. La divulgazione pubblica
4. La denuncia all'Autorità giudiziaria

Il legislatore ha disposto che debbano essere approntati all'interno degli enti cui si applica la normativa appositi "canali interni" per ricevere e trattare le segnalazioni. Il ricorso a questi canali viene incoraggiato, in quanto più prossimi all'origine delle questioni oggetto della segnalazione.

Nell'ottica di consentire di scegliere il canale di segnalazione più adeguato in funzione delle circostanze specifiche del caso, e quindi di garantire una più ampia protezione, si è prevista, al ricorrere di determinate condizioni, anche la divulgazione pubblica. Rimane naturalmente salvo il dovere di rivolgersi all'Autorità giudiziaria ove ne ricorrano i presupposti.

Il presente modello vuole, dunque, dettare una disciplina organizzativa relativa alla gestione delle segnalazioni interne, volta a garantire i soggetti segnalanti attraverso un'efficace tutela e protezione.

IL GESTORE DELLE SEGNALAZIONI

L'ente affida ad un unico soggetto, il RPCT, la gestione delle segnalazioni.

Non è prevista la possibilità di creare alcun gruppo di lavoro a supporto del RPCT.

Non è prevista la possibilità di gestione condivisa delle segnalazioni con altri enti.

Relativamente alle segnalazioni scritte mediante la piattaforma informatica, il fornitore del servizio riveste la qualifica di Responsabile del trattamento (art. 28 GDPR).

I CANALI DISPONIBILI

L'Ente incoraggia l'utilizzo del canale di segnalazione interno scritto mediante la piattaforma all'indirizzo

<https://comunediasiago.whistleblowing.it>

in considerazione delle elevate misure di sicurezza offerte dalla piattaforma stessa.

L'Ente rende disponibili anche altri canali interni: la conversazione telefonica o l'incontro diretto personale con il RPCT incaricato alla gestione delle segnalazioni.

IL CANALE INTERNO E LE MODALITÀ DI PRESENTAZIONE DELLE SEGNALAZIONI

Modalità di segnalazione scritta

Per le segnalazioni scritte, l'ente mette a disposizione una piattaforma informatica raggiungibile all'indirizzo <https://comunediasiago.whistleblowing.it>.

Dell'indirizzo internet per l'invio delle segnalazioni è dato risalto mediante pubblicazione sulla pagina web del sito istituzionale dedicata al whistleblowing.

La piattaforma fornisce al gestore delle segnalazioni la possibilità di rilasciare un avviso di ricevimento delle segnalazioni, di mantenere le interlocuzioni con la persona segnalante, di dare seguito alle segnalazioni ricevute, di fornire riscontri al segnalante.

Le misure di sicurezza offerte dalla piattaforma garantiscono la riservatezza di tutti i soggetti coinvolti (soggetto segnalante, facilitatore, persona coinvolta, soggetti menzionati) e del contenuto della segnalazione e della relativa documentazione, nonché il rispetto della disciplina sul trattamento dei dati personali.

Le misure di sicurezza sono dettagliatamente descritte sul sito del fornitore <https://www.whistleblowing.it/>

Al segnalante, la piattaforma dà la possibilità di:

- fornire o meno i propri dati identificativi

- scegliere tra quattro metodi di contatto per comunicare con l’RPCT: tramite piattaforma, indirizzo e-mail, telefono, altro da specificare a cura del segnalante

Al ricevimento di una segnalazione, la piattaforma invia un messaggio di notifica mediante posta elettronica alla casella del RPCT. Il messaggio non contiene alcun dato relativo alla segnalazione ma segnala unicamente la presenza di una nuova segnalazione.

Il gestore delle segnalazioni è tenuto ad effettuare la conseguente attività di accertamento.

A seguito della ricezione della segnalazione, l’RPCT farà una valutazione preliminare sulla segnalazione e potrà interagire con il soggetto segnalante, per richiedere chiarimenti o approfondimenti. Durante questa fase potrà consultare, qualora necessario, anche altri uffici o soggetti, pur sempre mantenendo riservata l’identità del segnalante e condividendo le minime informazioni necessarie allo scopo.

Modalità di segnalazione orale

Per le segnalazioni orali, il segnalante può utilizzare, alternativamente, la linea telefonica utilizzando l’interno del RPCT o l’incontro diretto, richiedendo un appuntamento direttamente al RPCT.

E’ escluso l’utilizzo di messaggistica vocale.

E’ esclusa la possibilità di registrare le conversazioni telefoniche.

La documentazione (appunti del RPCT o verbali) redatta a seguito consenso del segnalante è trattata con le stesse modalità e misure di sicurezza previste per le segnalazioni scritte non inviate tramite la piattaforma.

Segnalazione interna inviata a soggetto incompetente

Qualora la segnalazione interna (scritta o orale) sia presentata ad un soggetto diverso dal RPCT, laddove il segnalante dichiara espressamente di voler beneficiare delle tutele in materia *whistleblowing* o tale volontà sia desumibile dalla segnalazione, la segnalazione è considerata “segnalazione *whistleblowing*” e deve essere trasmessa, entro sette giorni dal suo ricevimento, al soggetto interno competente (l’RPCT), dando contestuale notizia della trasmissione alla persona segnalante.

In caso di segnalazione orale a soggetto incompetente, quest’ultimo dovrà invitare il segnalante a rivolgersi al RPCT.

La trasmissione della segnalazione al RPCT deve garantire la riservatezza di tutti i soggetti coinvolti e del contenuto della segnalazione e della relativa documentazione, nonché il rispetto della disciplina sul trattamento dei dati personali.

Diversamente, se il segnalante non ha dichiarato espressamente di voler beneficiare delle tutele, o detta volontà non sia desumibile dalla segnalazione, detta segnalazione è considerata quale segnalazione ordinaria.

ISTRUTTORIA, INOLTRO AD ORGANI PREPOSTI, ARCHIVIAZIONE

In tutte le fasi di gestione delle segnalazioni, l’RPCT adotta misure di sicurezza per garantire la riservatezza di tutti i soggetti coinvolti e del contenuto della segnalazione e della relativa documentazione, nonché il rispetto della disciplina sul trattamento dei dati personali.

ADEMPIMENTI E MISURE DI SICUREZZA

L'Ente garantisce i seguenti adempimenti:

- Pubblicazione sulla pagina web del sito istituzionale dedicata al whistleblowing dell'indirizzo internet della piattaforma per l'invio delle segnalazioni
- Pubblicazione sulla pagina web del sito istituzionale dedicata al whistleblowing dell'informativa completa contenente tutte le informazioni previste dagli artt. 13 e 14 GDPR
- Tenuta del registro delle attività di trattamento
- Adozione modello organizzativo privacy
- Definizione procedura per la gestione delle violazioni dei dati personali
- Adozione regolamento sull'utilizzo delle strumentazioni informatiche
- Redazione della valutazione d'impatto - DPIA

Devono essere garantite altresì le seguenti misure di sicurezza:

Misure di sicurezza per le segnalazioni scritte inviate tramite la piattaforma

- Accordo (art. 28 GDPR - Responsabile del trattamento) con il fornitore della piattaforma.
- Vedasi le misure di sicurezza pubblicate sul sito del fornitore <https://www.whistleblowing.it/>.
- Accesso esclusivo al gestionale da parte del RPCT.
- Casella di posta elettronica ricevente l'avviso di inoltro segnalazioni ad uso esclusivo del RPCT su dominio dell'ente.
- Attivazione autenticazione a due fattori al sistema di gestione.
- Utilizzo di password di autenticazione di elevata complessità.
- Stampa della documentazione transitata attraverso il canale informatico consentita solo se strettamente necessario per valutare la segnalazione.
- Download / Salvataggio files documentazione transitata attraverso il canale informatico solo se strettamente necessario per valutare la segnalazione. Cancellazione immediata di files salvati. Divieto di salvataggio files in aree condivise e/o sottoposte a backup e/o nel cloud. Svuotamento cestino dopo la cancellazione dei files.
- Accesso alla piattaforma e gestione delle segnalazioni in ambiente protetto.
- Adozione di template standard per la designazione del RPCT / incaricato alla gestione delle segnalazioni contenenti il richiamo alla necessità di eseguire il "passaggio di consegne" (credenziali di accesso e casella di posta associata all'applicativo) dal vecchio al nuovo incaricato.

Misure di sicurezza per le segnalazioni scritte non inviate tramite la piattaforma

- Deposito e custodia documenti in locali non accessibili e in armadi o cassetti non accessibili.

- Disposizioni scritte a tutto il personale circa la gestione delle segnalazioni presentate a soggetti diversi dal RPCT.

Misure di sicurezza per eventuali segnalazioni tramite e-mail

- Casella di posta elettronica ad uso esclusivo del RPCT.
- Stampa di eventuale documentazione inoltrata tramite e-mail consentita solo se strettamente necessario per valutare la segnalazione.
- Download / Salvataggio files solo se strettamente necessario per valutare la segnalazione. Cancellazione immediata del messaggio e di eventuali files salvati. Divieto di salvataggio files in aree condivise e/o sottoposte a backup e/o nel cloud. Svuotamento cestino dopo la cancellazione dei files.
- Invito al segnalante ad utilizzare i canali previsti dal modello di gestione.
- Adozione di template standard per la designazione del RPCT / incaricato alla gestione delle segnalazioni contenenti il richiamo alla necessità di eseguire il “passaggio di consegne” (credenziali di accesso alla casella di posta elettronica) dal vecchio al nuovo incaricato.

Misure di sicurezza per le segnalazioni orali tramite linea telefonica

- Conversazioni riservate in ambiente protetto.
- Deposito e custodia documentazione (appunti del RPCT / verbali) in locali non accessibili o in armadi o cassetti non accessibili.
- Disposizioni scritte a tutto il personale circa la gestione delle segnalazioni presentate a soggetti diversi dal RPCT.
- Divieto di registrazione delle conversazioni su supporto analogico o digitale.

Misure di sicurezza per le segnalazioni orali tramite incontro diretto

- Conversazioni riservate in ambiente protetto.
- Deposito e custodia documentazione (appunti del RPCT / verbali) in locali non accessibili o in armadi o cassetti non accessibili.
- Disposizioni scritte a tutto il personale circa la gestione delle segnalazioni presentate a soggetti diversi dal RPCT.
- Divieto di registrazione delle conversazioni su supporto analogico o digitale.

Misure di sicurezza relative al passaggio di consegne tra gestori delle segnalazioni

Il passaggio di consegne nella gestione delle segnalazioni riveste un ruolo cruciale all'interno del processo di whistleblowing, rappresentando una fase particolarmente delicata e di estrema importanza. Questo momento transitorio richiede attenzione e meticolosità in quanto influisce direttamente sulla continuità, l'integrità, la riservatezza delle informazioni e l'efficacia del sistema di gestione delle segnalazioni stesse.

Particolare attenzione deve concentrarsi in modo specifico sul canale informatico, poiché esso non solo rappresenta il metodo incoraggiato, ma si afferma come la scelta preferibile.

Per canali alternativi, come il colloquio orale, meno suscettibili a dettagli specifici in fase di passaggio, va garantita altrettanta precisione e affidabilità nei processi di gestione delle segnalazioni.

La piattaforma informatica selezionata richiede, durante la registrazione, l'inserimento di un indirizzo di posta elettronica, il quale diventa l'indirizzo predefinito per gli alert relativi alle segnalazioni.

IPOTESI 1:

Casella di posta con redirect al gestore in carica

Nel caso in cui la mail di contatto del sistema non sia direttamente associata al gestore delle segnalazioni, ma le comunicazioni giungano tramite un redirect, il passaggio di consegne segue le seguenti fasi:

1. Il gestore uscente coordina il processo con il nuovo responsabile, fornendo accesso al sistema.
2. Disattivazione autenticazione a due fattori.
3. Il gestore uscente trasferisce informazioni sulle indagini in corso e dati rilevanti al nuovo gestore.
4. L'Amministratore di Sistema modifica le impostazioni della casella di posta, reindirizzandola al nuovo gestore.
5. Il nuovo gestore verifica l'attivazione del redirect, inviando un messaggio di prova.
6. Riattivazione autenticazione a due fattori.

IPOTESI 2:

Casella di posta personale del gestore

Se la mail di contatto è direttamente associata al gestore in carica, il processo segue queste fasi:

1. Il gestore uscente coordina il processo con il nuovo responsabile, fornendo tutte le informazioni e le credenziali necessarie per accedere al sistema di gestione delle segnalazioni.
2. Il nuovo gestore disattiva l'autenticazione a due fattori e modifica la mail di contatto, inserendo la propria casella di posta personale.
3. Il nuovo gestore riaattiva l'autenticazione a due fattori.
4. Il gestore uscente trasferisce le informazioni sulle indagini in corso, e qualsiasi dato rilevante al nuovo gestore.

Comunicazione agli interessati

Durante il passaggio di consegne e successivamente, è essenziale comunicare in modo trasparente agli interessati che potrebbero presentare nuove segnalazioni o avere necessità di contatto. Le informazioni aggiornate saranno tempestivamente pubblicate sulla pagina web dedicata al whistleblowing sul sito istituzionale.

Misure di sicurezza comuni a tutte le segnalazioni

- Trattamento dati in ambiente protetto.

- Gestione delle segnalazioni esclusivamente a cura del RPCT, senza la creazione di alcun gruppo di lavoro.
- Utilizzo in fase di stampa della funzione “stampa protetta” in caso di utilizzo di stampanti condivise.
- Distruzione immediata di eventuali stampe al termine dell'utilizzo. Distruzione in ogni caso al termine del turno di lavoro.
- Utilizzo di distruggidocumenti.
- Aggiornamento automatico dei sistemi operativi.
- Firewall e antivirus aggiornato con l'attivazione di idonee regole di controllo del traffico a difesa di eventuali intrusioni abusive nel sistema.
- Formazione continua al RPCT, sia per quanto riguarda le norme sulla privacy sia alle procedure di sicurezza.
- Audit di conformità periodici con il DPO.
- Rispetto dei tempi di conservazione.
- Comunicazioni in fase istruttoria e alla chiusura dell'istruttoria stessa (ad ufficio personale, responsabili di area, Autorità Giudiziaria, Corte dei conti, ANAC) eseguite in busta chiusa, con consegna personale, tramite il servizio postale o tramite e-mail personale del RPCT, senza l'inserimento nell'eventuale protocollo di dati personali relativi ai soggetti da tutelare o ai contenuti della segnalazione.

MODALITÀ E TEMPI DI CONSERVAZIONE DEI DATI

I dati verranno conservati per tutto il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

L'INFORMATIVA ARTT. 13-14 GDPR

L'informativa ai sensi degli artt. 13-14 GDPR è resa disponibile agli interessati mediante pubblicazione sul sito web dell'ente, nella pagina dedicata al whistleblowing.

INFORMAZIONI DA INSERIRE SUL SITO

Sul sito web istituzionale dell'ente è inserito un collegamento ad una pagina dedicata all'istituto del whistleblowing.

Nella pagina sono inserite le seguenti informazioni/documenti:

- il collegamento alla piattaforma per l'effettuazione delle segnalazioni
- il collegamento alla piattaforma ANAC
- il presente modello
- l'informativa sul trattamento dei dati personali

- ulteriori informazioni riguardo alla disponibilità degli specifici canali di segnalazione offerti dall'ente, al fine di evitare l'utilizzo di canali alternativi non previsti
- ulteriori informazioni relative all'istituto del whistleblowing, eventualmente anche con collegamento alla pagina dedicata di ANAC
- le Linee Guida ANAC

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI - DPIA

L'ente ha redatto la valutazione di impatto - DPIA - per valutare il rischio e renderlo minimo per i diritti e le libertà degli interessati. Dalla DPIA condotta, il livello di rischio residuo per i diritti e le libertà degli interessati è risultato MEDIO BASSO, quindi accettabile.

Per quanto non previsto e/o specificato nel presente modello, si fa riferimento al D.Lgs. 10 marzo 2023, n. 24, e alle Linee Guida ANAC.