TRATTAMENTO DATI RELATIVI ALLE SEGNALAZIONI DI CONDOTTE ILLECITE (C.D. WHISTLEBLOWING)

DECRETO LEGISLATIVO 10 marzo 2023, n. 24 Attuazione della 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 e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

DATA PROTECTION IMPACT ASSESSMENT VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

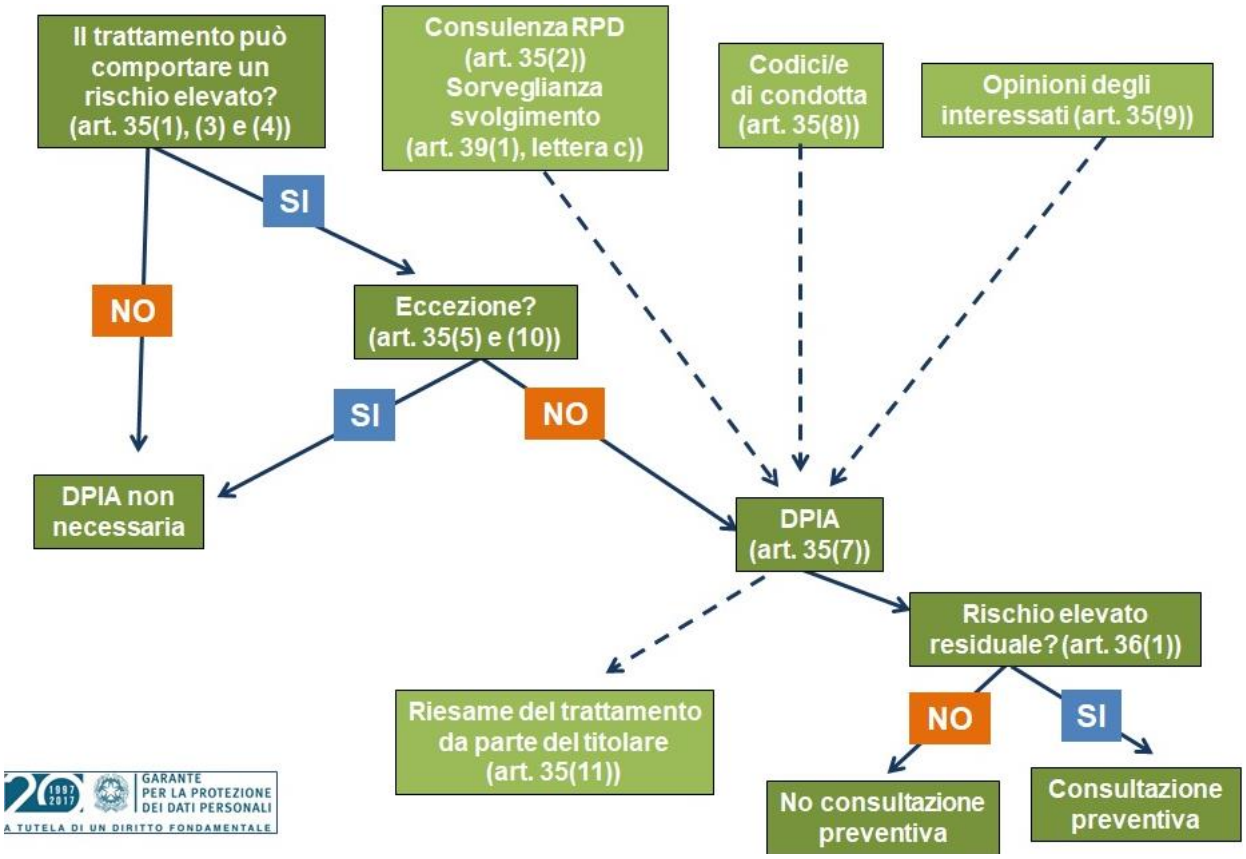
(art.35 Regolamento UE/2016/679 GDPR)

Titolare del trattamento	**Azienda Speciale Comuni Riuniti** ("ASCR"), con sede in Villagrande di Montecopiolo (RN), Piazza San Michele Arcangelo, n. 7, c.f. 02254180413, email comuniriuniti@libero.it, pec comuni.riuniti@pec.it
Responsabile del trattamento	PA33 S.r.l.

SOMMARIO

1. Premessa

L'art. 35 del Regolamento Europeo 679/2016 prevede che "quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".



Il presente documento rappresenta gli esiti della DPIA svolta nell'ambito del trattamento denominato Whistleblowing - di cui all'art. 54bis del D.Lgs. 165/2021 - effettuato da AZIENDA SPECIALE COMUNI RIUNITI "ASCR"

La valutazione di impatto si riferisce alla valutazione dei rischi in cui potrebbero incorrere le libertà ed i diritti dei cittadini dall'utilizzo della piattaforma informatica gratuita ed è stata svolta dal Titolare del trattamento con il supporto di PA33 S.r.l. quale Responsabile esterno del trattamento.

2. Fonti normative

- D. Lgs. n.24 del 10.3.2023;
- Regolamento UE n. 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
- D. Lgs. n. 196 del 30 giugno 2003 recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;
- Linee Guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679 adottate il 04 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017 dal Gruppo di Lavoro Articolo 29 per la Protezione dei Dati.

3. Definizioni

FONTE DI RISCHIO - Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (es. amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio.

GRAVITA' - La gravità rappresenta l'entità del rischio e dipende principalmente dalla natura pregiudizievole del potenziale impatto.

IMPATTO - L'impatto rappresenta il grado di gravità dell'incidente che comporta la compromissione della riservatezza, integrità e disponibilità dei trattamenti e dei dati ad essi relativi.

PROBABILITA' - La probabilità esprime la possibilità che un rischio si realizzi e dipende principalmente dal livello di vulnerabilità delle risorse di supporto quando sottoposte alle minacce e dalla capacità delle fonti di rischio di sfruttare tali vulnerabilità.

MINACCIA – La minaccia è l'evento potenziale, cagionato ovvero accidentale, che comporterebbe il danno all'interessato.

VULNERABILITA' – La vulnerabilità è l'elemento di debolezza presente all'interno del sistema informativo o informatico sfruttabile dalla minaccia per la produzione del danno.

MISURE DI SICUREZZA - Soluzioni organizzative, tecnologiche o procedurali messe in atto dal Titolare del trattamento per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Reg. UE 679/2016.

4. Contesto

4.1 Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento in esame riguarda le segnalazioni di illeciti, c.d. Whistleblowing, da parte di persone che operano nel contesto lavorativo di AZIENDA SPECIALE COMUNI RIUNITI "ASCR".

AZIENDA SPECIALE COMUNI RIUNITI "ASCR" intende adottare un canale informatico per consentire l'invio di una segnalazione in forma scritta, nonché un canale orale con numero telefonico.

La gestione delle segnalazioni attraverso il canale informatico avviene attraverso un applicativo fornito da PA33 S.r.l., in qualità di responsabile del trattamento, che si occupa della gestione del sistema di Whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.

I dati vengono forniti dal segnalante e vengono trattati dal titolare allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto della segnalazione e l'adozione dei conseguenti provvedimenti.

I dati personali sono trattati dal Responsabile del procedimento, ovvero dal gestore delle segnalazioni nominato dall'ente privato e designato al trattamento dei dati personali, poiché può avere accesso alle informazioni relative al segnalante.

Descrizione piattaforma Wb33 Whistleblowing

Il segnalante accede al link fornito ed effettua la registrazione, dichiarando i suoi dati identificativi e i suoi dati di contatto. Al termine della compilazione di tutti i campi, riceve un codice OTP sul numero di cellulare inserito per confermare l'iscrizione.

L'amministratore del servizio (soggetto individuato interno all'ente privato) riceve la richiesta di registrazione, verifica che i dati inseriti siano veritieri, ed abilita il soggetto all'utilizzo della piattaforma. L'amministratore del servizio individuato ha il solo compito di verificare le anagrafiche inserite, non può sapere in alcun modo se un utente ha effettuato o meno una segnalazione o se qualcuno ha mai inviato una segnalazione.

Il segnalante riceve una notifica di attivazione del suo account e, da questo momento, può eventualmente inviare una segnalazione, compilando il form proposto con le seguenti informazioni:

- Qualifica Servizio Attuale*
- Incarico (Ruolo) di Servizio Attuale*
- Unita Organizzativa e Sede di Servizio Attuale*
- Qualifica Servizio all'Epoca del Fatto Segnalato*
- Incarico (Ruolo) di Servizio all'Epoca del Fatto Segnalato*
- Unità Organizzativa e Sede di Servizio all'Epoca del Fatto*
- Ente coinvolto
- Periodo in cui si è verificato il Fatto*
- Data in cui si è verificato il Fatto
- Luogo fisico in cui si è verificato l'illecito/criticità*
- Soggetto che ha commesso il fatto (Nome, Cognome, Qualifica)*
- Eventuali soggetti privati coinvolti
- Eventuali imprese coinvolte
- Modalità con cui è venuto a conoscenza del fatto*
- Eventuali altri soggetti che possono riferire sul fatto
- (Nome, cognome, qualifica, recapiti)
- Area a cui può essere riferito il fatto
- Settore cui può essere riferito il fatto
- Descrizione del fatto*
- La condotta è illecita perchè…*

Una volta compilati tutti i campi obbligatori, riceve un codice OTP sul numero di cellulare per confermare l'invio.

Il software disaccoppia i dati della segnalazione dai dati del segnalante, conservandoli su server distinti, che saranno, poi, riaccoppiati solo su specifica richiesta tracciata da parte del Responsabile della gestione della segnalazione.

Il Responsabile riceve una notifica che lo avvisa della presenza di una nuova segnalazione da gestire. Accede alla sua area riservata e può gestire la segnalazione.

Di seguito le azioni che il Responsabile può eseguire dal suo account:

- visualizzare il documento SENZA i dati del segnalante visibili (questa azione è preceduta da un alert che raccomanda di non effettuare il download del documento, in modo da assicurarne la gestione solo all'interno del software);

- visualizzare gli eventuali allegati;

- visualizzare le informazioni relative all'identità del segnalante (questa azione è preceduta da due alert, per essere sicuri della volontà di accedere a tali informazioni);

- dialogare in maniera riservata con il segnalante per richiedere chiarimenti, aggiornamenti, ulteriori dettagli (il sw recapita i messaggi dal Responsabile al segnalante, senza che il Responsabile sappia a chi sono stati inviati - il segnalante riceve i messaggi nel proprio account, da cui può rispondere e inviare allegati);

- archiviare la segnalazione, selezionando la motivazione dal menù a tendina;

- prendere in carico la segnalazione, assegnandola all'ufficio/utente competente.

Gli uffici o gli utenti INTERNI all'ente privato, a cui assegnare la segnalazione, vengono "caricati" sulla piattaforma direttamente dal Responsabile che crea gli account di volta in volta necessari.

L'utente creato dal Responsabile riceve, per email, il link e le credenziali di accesso alla sua area riservata, in cui può visualizzare esclusivamente le segnalazioni che gli sono state assegnate.

Su tali segnalazioni, l'utente può:

- visualizzare il documento SENZA i dati del segnalante visibili (questa azione è preceduta da un alert che raccomanda di non effettuare il download del documento, in modo da assicurarne la gestione solo all'interno del software);

- visualizzare gli eventuali allegati;

- aggiungere dettagli da condividere con il Responsabile e con eventuali altri utenti coinvolti;

- visualizzare dettagli aggiunti dal Responsabile e da eventuali altri utenti coinvolti;

- chiudere la segnalazione con motivazione.

Per ogni segnalazione è disponibile un file log che viene automaticamente compilato dal software, in cui sono riportate tutte le azioni compiute da tutti i soggetti coinvolti nella gestione della segnalazione.

Ogni cambio di stato della segnalazione, viene notificato al segnalante, che è sempre aggiornato sullo stato di lavorazione della sua segnalazione.

Se la segnalazione necessita di gestione ESTERNA all'ente privato (ad esempio è necessario inviarla all'Autorità giudiziaria), il Responsabile può dichiarare al software che sta procedendo con l'inoltro esterno, aggiungendo tutti i dettagli utili a tenere traccia dell'attività svolta. Ciò al fine di alimentare il file log e di aggiornare il segnalante sullo stato di lavorazione.

Quali sono le responsabilità connesse al trattamento?

AZIENDA SPECIALE COMUNI RIUNITI "ASCR" -> Titolare del trattamento.

PA33 S.r.l.-> Responsabile del trattamento per la fornitura e la gestione dell'applicativo Wb33 Whistleblowing.

Ci sono standard applicabili al trattamento?

La piattaforma è coperta da certificato SSL ed utilizza solo protocolli sicuri TLS 1.3 per le connessioni.

Valutazione : Accettabile

4.2 Dati, processi e risorse di supporto

Quali sono i dati trattati?

In fase di registrazione alla piattaforma il segnalante fornisce i propri dati identificativi e di contatto. Una volta attivato l'account il segnalante può inviare la segnalazione compilando il form proposto ed inserendo le seguenti informazioni:

- Qualifica Servizio Attuale*
- Incarico (Ruolo) di Servizio Attuale*
- Unita Organizzativa e Sede di Servizio Attuale*
- Qualifica Servizio all'Epoca del Fatto Segnalato*
- Incarico (Ruolo) di Servizio all'Epoca del Fatto Segnalato*
- Unità Organizzativa e Sede di Servizio all'Epoca del Fatto*
- Ente coinvolto
- Periodo in cui si è verificato il Fatto*
- Data in cui si è verificato il Fatto
- Luogo fisico in cui si è verificato l'illecito/criticità*
- Soggetto che ha commesso il fatto (Nome, Cognome, Qualifica)*
- Eventuali soggetti privati coinvolti
- Eventuali imprese coinvolte
- Modalità con cui è venuto a conoscenza del fatto*
- Eventuali altri soggetti che possono riferire sul fatto
- (Nome, cognome, qualifica, recapiti)
- Area a cui può essere riferito il fatto
- Settore cui può essere riferito il fatto
- Descrizione del fatto*
- La condotta è illecita perchè…*

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

1. Attivazione della piattaforma accedendo al link fornito ed effettuando la registrazione.

2. Configurazione della piattaforma

3. Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte del Responsabile della gestione.

4. Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore.

Quali sono le risorse di supporto ai dati?

I dati sono archiviati in modalità logica all'interno di un *DB* ed utilizzati con un *DBMS* relazionale open source. I dati sono cifrati con algoritmo AES 256 con chiave simmetrica. Il database è replicato in backup con ciclicità giornaliera e *retention* di 3 copie su due sistemi.

Valutazione : Accettabile

5. Principi Fondamentali

5.1. Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento avviene con lo scopo specifico di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

I dati non vengono trattati per ulteriori finalità incompatibili con il predetto scopo.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

I dati personali sono trattati dal Responsabile della gestione delle segnalazioni, nell'esecuzione dei compiti allo stesso affidati, con particolare riferimento al compito di accertare eventuali illeciti segnalati, ciò nell'interesse dell'integrità della nostra organizzazione ed in adempimento di un obbligo di legge (D.lgs. n.24/2023)

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

La piattaforma è strutturata, fin dalla fase di progettazione, in modo tale da richiedere al segnalante esclusivamente i dati personali in misura proporzionata e non eccedente, necessari e pertinenti rispetto alla finalità perseguita.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

L'aggiornamento dei dati è a cura degli utenti registrati attraverso l'accesso alla propria area riservata.

Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati vengono conservati fino alla durata del servizio di segnalazione. Al termine del periodo di utilizzo, le informazioni vengono eliminate automaticamente dalla base dati, senza alcuna possibilità di ripristino

Valutazione : Accettabile

5.2 Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

La soluzione offre la possibilità al Titolare del trattamento di includere l'informativa sui dati personali e di renderla agli interessati prima dell'accesso alla piattaforma

Valutazione : Accettabile

Come si ottiene il consenso degli interessati?

Non è applicabile alla fattispecie

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati possono presentare una istanza per l'esercizio dei propri diritti all'Ente, nei limiti di quanto previsto dall'art. 2 undecies del D.Lgs. n.196 del 30 giugno 2003, mediante e-mail o pec, oppure mediante lettera raccomandata.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati possono presentare una istanza per l'esercizio dei propri diritti all'Ente nei limiti di quanto previsto dall'art. 2 undecies del D.Lgs. n.196 del 30 giugno 2003, mediante e-mail o pec, oppure mediante lettera raccomandata

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono presentare una istanza per l'esercizio dei propri diritti all'Ente nei limiti di quanto previsto dall'art. 2 undecies del D.Lgs. n.196 del 30 giugno 2003, mediante e-mail o pec, oppure mediante lettera raccomandata.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Si, è stato sottoscritto l'accordo sulla protezione dei dati ai sensi dell'art.28 GDPR con PA33 S.r.l.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Euroepa. Non esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

Valutazione : Accettabile

6. Rischi

6.1. Misure esistenti o pianificate

- **Crittografia**

La piattaforma utilizza un protocollo di crittografia che garantisce la sicurezza e confidenzialità tecnologica del processo di segnalazione, ovvero delle informazioni che transitano attraverso la piattaforma, attraverso la crittografia con algoritmo di ultima generazione *AES* 256 con chiave simmetrica.

Valutazione : Accettabile

- **Anonimizzazione**

La piattaforma è provvista di un servizio di comunicazione interno che consente lo scambio di messaggi e documenti tra segnalante e Responsabile in maniera totalmente anonima. Le comunicazioni avvengono esclusivamente attraverso la piattaforma, che recapita i messaggi senza rendere visibile il mittente e il destinatario, ma avendo, come unico riferimento, l'ID della segnalazione.

Valutazione : Accettabile

- **Partizionamento**

Il software disaccoppia i dati della segnalazione dai dati del segnalante, conservandoli su server distinti, che saranno, poi, riaccoppiati solo su specifica richiesta tracciata da parte del RPCT. Tutte le anagrafiche presenti nella piattaforma, attraverso strumenti informatici, sono disaccoppiate

dai dati correlati: le segnalazioni sono collegate all'anagrafica attraverso codice non raggiungibile dalle utenze di gestione segnalazioni.

Valutazione : Accettabile

- **Tracciabilità**

Garanzia di non tracciabilità del segnalante:

l'accesso alla piattaforma avviene tramite protocollo sicuro https che consente di garantire la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione mediante l'impiego di strumenti di anonimizzazione dei dati di navigazione.

L'Ente privato dovrà verificare le impostazioni di sicurezza dei propri sistemi firewall e proxy eventualmente presenti.

Tracciamento dell'attività:

l'attività di tracciamento degli utenti del sistema viene effettuata nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione. Le informazioni relative ai log sono protette da accessi non autorizzati e vengono conservate per un termine congruo rispetto alle finalità di tracciamento. Non vengono svolte attività di tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante. Il tracciamento è effettuato esclusivamente al fine di garantire la correttezza e la sicurezza del trattamento dei dati.

I log sono accessibili esclusivamente al Responsabile e ai soggetti autorizzati e solo dopo aver effettuato l'accesso alla propria area di gestione.

Valutazione : Accettabile

- **Controllo degli accessi logici**

La modalità di accesso alla piattaforma prevede un sistema di autenticazione informatica basata su tecniche di strong authentication: per effettuare la registrazione e per inviare una segnalazione è richiesta conferma attraverso un codice OTP.

Sulla base di valutazioni effettuate caso per caso anche in ragione delle specificità del contesto tecnologico, della dimensione dell'ente titolare, del numero di utenti e della ricorrenza di specifiche situazioni di criticità, è possibile implementare ulteriori misure di sicurezza.

Valutazione : Accettabile

- **Archiviazione**

I dati sono archiviati in modalità logica all'interno di un DB ed utilizzati con un DBMS relazionale open source. I dati sono cifrati con algoritmo AES 256 con chiave simmetrica. Il database è replicato in backup con ciclicità giornaliera e retention di 3 copie su due sistemi

Valutazione : Accettabile

- **Tutela della riservatezza del segnalante**

L'identità del segnalante può essere conosciuta, al termine della fase di accertamento, esclusivamente dal Responsabile.

E' inoltre preclusa la possibilità di visualizzare l'identità del segnalante ai soggetti terzi coinvolti nelle attività di accertamento e di accesso alla segnalazione.

Tali soggetti hanno accesso esclusivamente alle informazioni della segnalazione, prive di riferimenti a dati personali.

Valutazione : Accettabile

- **Informativa sul trattamento dei dati personali**

La soluzione offre la possibilità al Titolare del trattamento di includere l'informativa sui dati personali e di renderla agli interessati prima dell'accesso alla piattaforma.

Valutazione : Accettabile

- **Identificazione del segnalante**

Ogni segnalazione è identificata con il rilascio di un codice univoco.

Il sistema registra la data e l'ora di ricezione della segnalazione, il codice univoco, ed invia le stesse informazioni al segnalante.

Le informazioni rimangono stabilmente associate alla segnalazione.

Valutazione : Accettabile

- **Tutela della riservatezza del contenuto della segnalazione**

L'accesso alle informazioni contenute nella segnalazione, quali la documentazione ad essa allegata nonché all'identità di eventuali soggetti segnalati, è consentito esclusivamente ai soggetti autorizzati e previsti nell'iter procedurale.

Valutazione : Accettabile

- **Segregazione dei dati e delle informazioni**

Al momento dell'inizio della procedura di segnalazione, l'applicativo avvia la separazione del contenuto della segnalazione dall'identità del segnalante.

La procedura di abbinamento dei dati viene effettuata automaticamente al momento della richiesta del Responsabile di conoscere l'identità del segnalante

Valutazione : Accettabile

- **Accesso selettivo ai dati delle segnalazioni**

La piattaforma assicura l'accesso selettivo ai dati delle segnalazioni da parte dei diversi soggetti autorizzati al trattamento. Prevede procedura per l'assegnazione da parte del Responsabile della trattazione di specifiche segnalazioni all'eventuale personale di supporto. Il Responsabile assegna la segnalazione esclusivamente a soggetti da lui individuati e autorizzati.

Ciascun soggetto può accedere esclusivamente ai dati delle segnalazioni che gli sono state assegnate.

Valutazione : Accettabile

- **Accesso all'identità del segnalante esclusivamente da parte del Responsabile della gestione delle segnalazioni**

L'accesso all'identità del segnalante è consentita esclusivamente al Responsabile della gestione delle segnalazioni dietro espresso consenso del "custode" dell'identità dal segnalante.

La figura del custode dell'identità non è obbligatoria.

In questo caso, il Responsabile della gestione delle segnalazioni coincide con il custode dell'identità. Il Responsabile è l'unico soggetto a poter accedere, su specifica richiesta tracciata dal sistema, all'identità del segnalante.

Valutazione : Accettabile

- **Sicurezza delle notifiche**

Nell'invio di messaggi sulla casella di posta elettronica individuale che l'amministrazione o l'ente ha assegnato al Responsabile della gestione delle segnalazioni (es. in caso di variazione dello stato di avanzamento dell'istruttoria, riscontro del segnalante a una richiesta di integrazione, riscontro del segnalante a una richiesta di consenso a rivelare la propria identità nell'ambito di un procedimento disciplinare, ecc.), la piattaforma non trasmette informazioni riferite all'identità del segnalante o all'oggetto della segnalazione.

Valutazione : Accettabile

- **Stato dell'istruttoria**

L'applicativo consente al segnalante di verificare, in qualsiasi momento, lo stato di avanzamento dell'istruttoria.

Il segnalante viene, inoltre, avvisato tramite canali sms ed email ad ogni cambio di stato della segnalazione.

Valutazione : Accettabile

- **Disponibilità ed integrità dei dati**

Tramite l'applicazione è consentita, in qualsiasi momento, la fruibilità della documentazione custodita, ad es. al fine di evitare il download o, soprattutto, la stampa della stessa.

Valutazione : Accettabile

- **Policy: Norme comportamentali**

Al fine di consentire l'uso consapevole e sicuro della piattaforma, sono rese al personale dell'Ente, le indicazioni da seguire per l'invio e la gestione della segnalazione. Tali informazioni, trasmesse anche attraverso eventi di istruzione e formazione, sono da considerarsi requisiti minimi di buon comportamento. Tra questi, è suggerita: la rimozione dei riferimenti all'identità del segnalante dalla segnalazione e dai suoi allegati; l'utilizzo del canale informatico per tutte le comunicazioni successive da inviare all'Ente

Valutazione : Accettabile

- **Procedura per il segnalante con istruzioni sulle modalità di segnalazioni consentite**

Il "whistleblower", ovvero il segnalante ha a disposizione una procedura sotto forma di istruzione con la quale viene indirizzato sulle modalità di segnalazioni consentite.

Valutazione : Accettabile

- **Sicurezza delle credenziali di accesso**

Le password utente sono validate nella loro complessità secondo le best practices attuali e con richiesta semestrale di aggiornamento.

Per l'accesso lato segnalante è prevista autenticazione a due fattori.

Valutazione : Accettabile

- **Minimizzazione dei dati personali**

La piattaforma è strutturata, fin dalla fase di progettazione, in modo tale da richiedere al segnalante esclusivamente i dati personali in misura proporzionata e non eccedente, necessari e pertinenti rispetto alla finalità perseguita

Valutazione : Accettabile

- **Backup**

I dati sono archiviati in modalità logica all'interno di un DB ed utilizzati con un DBMS relazionale open source. I dati sono cifrati con algoritmo AES 256 con chiave simmetrica. Il database è replicato in backup con ciclicità giornaliera e retention di 3 copie su due sistemi.

Valutazione : Accettabile

- **Sicurezza dei canali informatici**

La piattaforma utilizza un protocollo di crittografia che garantisce la sicurezza e confidenzialità tecnologica del processo di segnalazione attraverso la crittografia con algoritmo di ultima generazione AES 256 con chiave simmetrica.

Valutazione : Accettabile

- **Lotta contro il malware**

I funzionari abilitati all'accesso sono individuati dall'ente.

La piattaforma è coperta da certificato SSL ed utilizza solo protocolli sicuri TLS 1.3 per le connessioni. L'architettura complessiva è protetta da firewall perimetrali che consentono l'accesso solo a servizi presidiati.

Valutazione : Accettabile

- **Contratto con il responsabile del trattamento**

E' stato definito il contratto con il responsabile del trattamento PA33 S.r.l.

Valutazione : Accettabile

- **Formazione dell'Organo di gestione**

Formazione del Responsabile della gestione delle segnalazioni e del personale che può essere coinvolto nell'istruttoria.

Valutazione : Accettabile

- **Nomine agli autorizzati**

I soggetti autorizzati ad accedere ai dati sono individuati, appositamente autorizzati ed istruiti

Valutazione : Accettabile

6.2 Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti psicologici e materiali

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Fonti umane interne

Quali sono le fonti di rischio?

Fonti umane interne: dipendente che usa la vicinanza al sistema o i suoi privilegi ed opera in maniera intenzionale o negligente per scarsa sensibilizzazione.

Accesso o sottrazione di documenti non conservati adeguatamente.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Formazione dell'Organo di gestione, Policy: Norme comportamentali, Anonimizzazione, Partizionamento, Tracciabilità, Controllo accessi logici, Tutela segretezza del segnalante, Tutela della riservatezza del contenuto della segnalazione, Accesso selettivo ai dati delle segnalazioni, Accesso ai dati del segnalante da parte del solo Responsabile delle segnalazioni, Nomine autorizzati ed istruzioni sul trattamento.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Significativo

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitato

Valutazione : Migliorabile

6.3. Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti psicologici e materiali

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Fonti umane interne

Quali sono le fonti di rischio?

Fonti umane interne: evento doloso

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Backup, Formazione dell'Organo di gestione, Policy: Norme comportamentali, Anonimizzazione, Partizionamento, Tracciabilità, Controllo accessi logici, Tutela segretezza del segnalante, Tutela della riservatezza del contenuto della segnalazione, Accesso selettivo ai dati delle segnalazioni, Accesso ai dati del segnalante da parte del solo Responsabile delle segnalazioni.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Significativo

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitato

Valutazione : Accettabile

6.4. Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Impatti psicologici e materiali

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Virus, Errore umano, Evento doloso

Quali sono le fonti di rischio?

Fonti non umane: codice malevolo di origine sconosciuta, Fonti umane interne ed esterne

Accesso o sottrazione di documenti non conservati adeguatamente.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Partizionamento, Tracciabilità, Backup, Controllo degli accessi logici, Archiviazione, Segregazione dei dati e delle informazioni, Sicurezza credenziali di accesso, Sicurezza dei canali informatici, Lotta contro il malware, Contratto con Responsabile esterno.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Significativo

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitato

Valutazione : Migliorabile

7. Piano d'azione

Principi fondamentali

Il flusso dei dati potrebbe fuoriuscire dal portale in caso di attività istruttorie utili a dar seguito alle segnalazioni, comprensive di audizioni e/o acquisizioni documentali.

Non solo, la stessa modalità di segnalazione orale potrebbe portare alla redazione di documenti comprovanti l'identità dell'interessato piuttosto che dei segnalati o terzi.

Pertanto i dati personali possono non essere contenuti esclusivamente all'interno della piattaforma, ma circolare materializzati o dematerializzati all'interno dell'organizzazione.

Conseguentemente, se il documento cartaceo non viene adeguatamente protetto, i dati sono esposti a rischi, quali l'accesso illegittimo ai dati e la perdita di dati.

Piano d'azione / misure correttive

Rischi

Accesso illegittimo ai dati

Commento di valutazione :

La minaccia è contenibile con l'adozione di misure per la sicurezza dei documenti cartacei

Piano d'azione / misure correttive :

Cassaforte o armadio in metallo con chiusura a chiave dove conservare la documentazione con accesso consentito solo al soggetto autorizzato.

Consenso del segnalante per la verbalizzazione della segnalazione come stabilito dal D. Lgs. n.24 del 10.3.2023.

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)**?**

Limitato
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)**?**

Limitato

Rischi

Perdita di dati

Commento di valutazione :

La minaccia è contenibile con l'adozione di misure per la sicurezza dei documenti cartacei

Piano d'azione / misure correttive :

Cassaforte o armadio in metallo con chiusura a chiave dove conservare la documentazione con accesso consentito solo al soggetto autorizzato.

Consenso del segnalante per la verbalizzazione della segnalazione come stabilito dal D. Lgs. n.24 del 10.3.2023.

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Perdita di dati)?

Limitato
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Perdita di dati)?

Limitato

8. Parere del DPO/RPD

Non applicabile. Non presente il DPO.

9. Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non è stato ritenuto necessario acquisire il parere dei potenziali interessati, anche in considerazione degli esiti della presente valutazione.