

Data Protection Impact Assessment

Comune di Sant'Agello

Revisione e aggiornamento della DPIA relativa al sistema di segnalazione di illeciti (Whistleblowing)

Codice documento: DPIA-WB-SA-REV.01

Versione: 2.0 – Revisione

Data documento: 12 / 03 / 2026

Il Sindaco:
Dott. Antonino Coppola

Premessa.

La presente Valutazione d'Impatto sulla Protezione dei Dati (DPIA) costituisce una revisione e aggiornamento della precedente DPIA relativa al trattamento di dati personali effettuato attraverso la piattaforma informatica di gestione delle segnalazioni di illeciti (whistleblowing) adottata dal Comune di Sant'Agnello.

L'aggiornamento del documento si inserisce in un'ottica di monitoraggio continuo della conformità del trattamento alla normativa vigente in materia di protezione dei dati personali, nonché di adeguamento alle evoluzioni organizzative, normative e tecnologiche intervenute nel tempo. In particolare, la revisione tiene conto delle verifiche periodiche effettuate sul sistema, delle attività di aggiornamento e manutenzione evolutiva della piattaforma software e delle esigenze di rafforzamento complessivo del presidio di compliance del trattamento.

La presente DPIA conferma pertanto l'impianto generale della valutazione precedentemente adottata, aggiornandone l'analisi dei rischi, la descrizione delle misure tecniche e organizzative e il quadro di riferimento normativo, al fine di garantire il mantenimento di un adeguato livello di protezione dei dati personali trattati nell'ambito della procedura di whistleblowing dell'Ente.

Nome del DPO/RPD

Fabrizio Corona

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

All'esito della valutazione effettuata, si ritiene che il trattamento possa essere implementato in quanto le finalità perseguite risultano legittime, determinate e coerenti con gli obblighi normativi in materia di prevenzione della corruzione e tutela dei segnalanti previsti dal D.lgs. 24/2023 e dal Regolamento (UE) 2016/679. Le misure tecniche e organizzative adottate appaiono idonee a garantire un adeguato livello di sicurezza dei dati personali trattati, in particolare sotto il profilo della riservatezza dell'identità del segnalante, della tracciabilità delle operazioni effettuate sulla piattaforma e della limitazione degli accessi ai soli soggetti autorizzati. Alla luce delle misure implementate e della valutazione dei rischi effettuata, il rischio residuo per i diritti e le libertà degli interessati può essere considerato accettabile e proporzionato rispetto alle finalità del trattamento.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non è stata effettuata una consultazione degli interessati nell'ambito della presente valutazione d'impatto. Tale scelta risulta giustificata dalla natura del trattamento, che riguarda la gestione di segnalazioni di illeciti e presuppone specifiche esigenze di riservatezza e protezione dell'identità del segnalante. Una consultazione preventiva degli interessati potrebbe infatti compromettere l'efficacia del sistema di segnalazione e pregiudicare le finalità di prevenzione e contrasto degli illeciti perseguite dalla normativa di riferimento. Il trattamento è pertanto disciplinato mediante specifiche misure organizzative e tecniche volte a garantire la tutela dei diritti e delle libertà degli interessati, in conformità al Regolamento (UE) 2016/679 e al D.lgs. 24/2023.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento in considerazione riguarda la gestione delle segnalazioni di illeciti o irregolarità, disciplinate dalla procedura di whistleblowing adottata dal Comune di Sant'Agnello. La procedura si inserisce nell'ambito della normativa nazionale e comunitaria che tutela i segnalanti, ovvero le persone che, venute a conoscenza di comportamenti illeciti o irregolari nell'ambito del loro lavoro, decidono di segnalarli alle autorità competenti. La piattaforma utilizzata per raccogliere queste segnalazioni è denominata **"Whistleblowing Intelligente"**, un sistema basato su un servizio SaaS (Software as a Service) che consente di raccogliere segnalazioni sia in forma anonima che identificata. Le segnalazioni possono essere inviate tramite una piattaforma informatica, ma anche mediante segnalazioni vocali o orali su appuntamento, a seconda della preferenza del segnalante.

Il trattamento può riguardare dati personali relativi ai segnalanti, ai soggetti segnalati e ad eventuali altri soggetti coinvolti nella segnalazione. Le categorie di dati trattati possono comprendere dati identificativi e di contatto, dati relativi al rapporto di lavoro o di collaborazione con l'ente e, ove strettamente necessari ai fini della gestione della segnalazione, informazioni relative a presunte condotte illecite.

Le finalità del trattamento dei dati raccolti riguardano principalmente la gestione delle segnalazioni, la verifica dell'eventuale violazione delle normative, e l'attuazione di misure protettive per tutelare il segnalante da eventuali ritorsioni. La piattaforma assicura la riservatezza del segnalante e dei dati, rispettando gli obblighi previsti dal **D.lgs. 24/2023** (che recepisce la Direttiva (UE) 2019/1937) in tema di protezione dei whistleblower. I risultati attesi da questa procedura sono la corretta gestione e trattazione delle segnalazioni, la

protezione dei diritti dei segnalanti e la promozione della legalità all'interno dell'amministrazione comunale. L'obiettivo è garantire che ogni segnalazione venga trattata con riservatezza, e che venga presa una decisione appropriata in merito all'eventuale azione correttiva da intraprendere. L'uso della piattaforma garantisce che le segnalazioni vengano gestite in modo sicuro e tracciato, rispettando la privacy del segnalante e delle persone coinvolte.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità connesse al trattamento sono distribuite tra diversi soggetti coinvolti nel processo.

Il **Titolare del trattamento** è il **Comune di Sant'Agnello**, che è l'entità giuridica principale che gestisce e definisce la politica del trattamento dei dati personali, prendendo decisioni finali sul trattamento e garantendo la conformità alla normativa.

All'interno del Comune, l'**RPCT** (Responsabile della prevenzione della corruzione e della trasparenza) ha il compito di gestire il processo operativo delle segnalazioni e garantire che vengano seguite tutte le procedure interne per rispondere alle segnalazioni ricevute.

Il **Responsabile della protezione dei dati (DPO)**, nominato dal Comune, è incaricato di supervisionare il rispetto della normativa sulla protezione dei dati personali e fornire supporto nella gestione delle problematiche relative alla privacy.

Inoltre, la piattaforma "Whistleblowing Intelligente" è gestita dalla società **Tecnolink S.r.l.**, che funge da **Responsabile del trattamento** ai sensi dell'art. 28 del GDPR. Tecnolink è incaricata della gestione tecnica della piattaforma e dei dati personali relativi alle segnalazioni, ma opera sotto le istruzioni del Comune di Sant'Agnello.

Ci sono standard applicabili al trattamento?

Per quanto riguarda gli **standard applicabili al trattamento**, il sistema adottato dal Comune di Sant'Agnello segue gli standard stabiliti dal **GDPR (Regolamento (UE) n. 2016/679)**, che garantisce la protezione dei dati personali. In particolare, il trattamento dei dati deve rispettare il principio di **privacy by design and by default**, che implica che le misure di protezione dei dati siano integrate fin dalla progettazione della piattaforma. Inoltre, vengono rispettati gli standard di **cybersecurity**, con la piattaforma registrata nel **Cloud Marketplace dell'Autorità per la Cybersicurezza Nazionale (ACN)**, che ne certifica la sicurezza e l'affidabilità. La piattaforma implementa misure tecniche come la **crittografia dei dati**, la **segretezza dei dati identificativi del segnalante**, e l'**accesso limitato** ai dati da parte solo di soggetti autorizzati, in conformità con le Linee guida ANAC e le normative sulla protezione dei dati. Il sistema assicura anche l'**audit trail**, ovvero la **tracciabilità degli accessi e delle operazioni effettuate sui dati**.

In relazione agli standard applicabili al trattamento, è opportuno segnalare che, oltre alla conformità al **Regolamento (UE) 2016/679 (GDPR)** e al **D.lgs. 24/2023**, il Comune di Sant'Agnello ha formalmente adottato un **Atto Organizzativo di Attuazione della Disciplina del Whistleblowing**, approvato con **deliberazione di Giunta Comunale n. 146 del 12/12/2023**.

Tale documento rappresenta uno **standard interno vincolante**, che definisce puntualmente ruoli, responsabilità, modalità operative e misure di sicurezza da applicare al trattamento dei dati personali nell'ambito della gestione delle segnalazioni. L'atto si configura come parte integrante del sistema di compliance dell'ente, in attuazione delle **Linee guida ANAC n. 469/2021**, e garantisce un presidio organizzativo strutturato e trasparente in materia di whistleblowing, rafforzando l'affidabilità del trattamento sotto il profilo sia giuridico che procedurale.

Valutazione : Accettabile

Commento di valutazione :

Sulla base delle informazioni disponibili, le misure tecniche e organizzative implementate risultano adeguate e proporzionate rispetto ai rischi individuati, rendendo il trattamento accettabile sotto il profilo della protezione dei dati personali.

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati personali trattati possono essere suddivisi in più categorie, a seconda della modalità di segnalazione e del contenuto stesso della segnalazione. Vengono trattati **dati identificativi del segnalante** (qualora non anonimo), **dati delle persone coinvolte o menzionate nella segnalazione**, **dati relativi ai fatti segnalati**, nonché eventuali **categorie particolari di dati ai sensi dell'art. 9 del GDPR** (ad esempio dati relativi a opinioni politiche, stato di salute, convinzioni religiose o appartenenza sindacale) e **dati relativi a condanne penali o reati** (art. 10 GDPR), se pertinenti. In aggiunta, dati relativi alla registrazione della voce del segnalante, ove la segnalazione avvenga tramite canale vocale.

Il periodo di conservazione previsto è pari a **5 anni dalla comunicazione dell'esito finale della segnalazione**, come disposto dall'art. 14 del D.lgs. 24/2023 e come riportato nell'atto organizzativo interno. I dati non pertinenti o manifestamente inutili vengono cancellati tempestivamente. I **destinatari dei dati** possono essere, laddove necessario, l'Autorità Nazionale Anticorruzione (ANAC), l'Autorità Giudiziaria, la Corte dei conti o l'Ufficio Provvedimenti Disciplinari, a seconda della natura e dell'esito della segnalazione. I **soggetti autorizzati all'accesso** ai dati sono esclusivamente il **Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT)**, nonché gli eventuali collaboratori da lui formalmente designati e istruiti. Nessun altro soggetto può accedere ai dati, né è consentita la diffusione degli stessi. In caso di accesso ai dati identificativi del segnalante, la piattaforma registra la motivazione e notifica l'avvenuto accesso al segnalante stesso.

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

Il ciclo di vita dei dati segue un processo articolato, tracciato dalla piattaforma **Whistleblowing Intelligente**, strutturato come segue:

- **Raccolta dei dati:** avviene tramite piattaforma web sicura, accesso tramite piattaforma web sicura che consente l'invio della segnalazione sia in forma identificata sia anonima. Il segnalante può allegare documenti, registrazioni vocali o inserire riferimenti a terzi. In alternativa, la segnalazione può essere acquisita oralmente (telefono o incontro diretto).
- **Registrazione e protocollazione:** il sistema assegna automaticamente un ID univoco e registra data e ora della segnalazione, impedendo modifiche o cancellazioni.
- **Presa in carico:** il RPCT riceve una notifica della segnalazione ed è l'unico soggetto abilitato a leggerla entro 7 giorni. In caso di necessità, può affidarne la gestione a un collaboratore interno.
- **Valutazione preliminare:** vengono esaminati i presupposti formali per la ricevibilità (contenuto circostanziato, riferibilità all'Ente, pertinenza).
- **Istruttoria:** si sviluppano eventuali richieste di chiarimento al segnalante, consultazioni documentali e raccolta di ulteriori elementi. Tutte le attività sono tracciate nella piattaforma.
- **Chiusura della segnalazione:** al termine dell'istruttoria (entro 90 giorni), si redige un verbale interno nella piattaforma, che può condurre all'archiviazione o alla trasmissione ad ANAC, autorità giudiziaria o Corte dei conti.
- **Archiviazione:** i dati restano disponibili nella piattaforma per un periodo massimo di 5 anni. Anche dopo la chiusura, la chat asincrona tra segnalante e RPCT resta attiva per eventuali aggiornamenti o segnalazioni di ritorsioni.
- **Cancellazione:** decorso il termine, i dati vengono eliminati in conformità alla policy di retention.

Quali sono le risorse di supporto ai dati?

Le risorse di supporto al trattamento comprendono sia componenti tecniche che organizzative. I dati sono ospitati all'interno della piattaforma **Whistleblowing Intelligente**, basata su infrastruttura cloud **Microsoft Azure**, localizzata in data center situati nell'Unione Europea (Paesi Bassi e Irlanda). La protezione dei dati è garantita tramite crittografia dei database e dei documenti, autenticazione forte degli utenti autorizzati, segregazione delle informazioni riservate, firewall e sistemi antivirus. I sistemi operativi impiegati sono virtualizzati e accessibili unicamente tramite VPN. Il back-up delle macchine virtuali avviene ogni 4 ore, con retention di 15 giorni e disaster recovery cross-region attivo. Il software è conforme agli standard di sicurezza definiti dal **Cloud Marketplace dell'ACN**, ed è registrato anche presso lo **STAR Registry della Cloud Security Alliance**.

Le risorse umane coinvolte nel trattamento sono i soggetti formalmente incaricati dal Titolare, in particolare il **RPCT**, i collaboratori autorizzati, e il **DPO** in funzione di vigilanza. I supporti fisici (es. cartacei) sono esclusi dalla procedura, salvo segnalazioni eccezionali ricevute con mezzi tradizionali, che vengono protocollate in registri riservati e trattate con le stesse garanzie di riservatezza e integrità previste per il canale informatico.

Valutazione : Accettabile

Commento di valutazione :

Alla luce delle misure tecniche e organizzative implementate, il trattamento risulta adeguatamente presidiato e i rischi individuati possono ritenersi accettabili rispetto alle finalità perseguite.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

gli scopi del trattamento effettuato dal Comune di Sant'Agnello nell'ambito della procedura whistleblowing sono pienamente **specifici, espliciti e legittimi**. Il trattamento dei dati personali ha come finalità principale quella di consentire la ricezione, la gestione e l'istruttoria delle segnalazioni di illeciti o irregolarità, nel rispetto della normativa nazionale (D.lgs. 24/2023), del diritto europeo (Direttiva (UE) 2019/1937) nonché con le Linee guida ANAC in materia di gestione delle segnalazioni di illeciti e con le misure organizzative adottate dall'Ente nell'ambito del proprio sistema di prevenzione della corruzione e della trasparenza.. Si tratta di una finalità chiaramente definita e collegata a un obbligo giuridico, quale la tutela dell'interesse pubblico, l'integrità dell'amministrazione e la protezione delle persone che segnalano violazioni di legge. Inoltre, le finalità sono esplicitate nel testo dell'atto organizzativo adottato dall'ente (delibera di Giunta n. 146/2023), nonché nell'informativa fornita al momento della segnalazione, e sono accessibili anche tramite i canali ufficiali dell'amministrazione.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La legittimità delle finalità deriva dalla necessità di adempiere a obblighi legali specifici previsti dalla normativa anticorruzione e in materia di protezione dei whistleblower. In particolare, la base giuridica che rende lecito il trattamento è rappresentata, ai sensi dell'art. 6, par. 1 lett. **c)** del GDPR, dall'adempimento di un **obbligo legale** al quale è soggetto il Titolare, ovvero il Comune di Sant'Agnello, in quanto amministrazione pubblica tenuta ad attivare canali di segnalazione sicuri ed efficaci. Per il trattamento di eventuali **categorie particolari di dati** (art. 9 GDPR), si applicano le lettere **b)** e **g)** dello stesso articolo, poiché il trattamento è necessario per adempiere a obblighi nel campo del diritto del lavoro e per motivi di interesse pubblico rilevante. Per le segnalazioni effettuate oralmente tramite canali vocali, il trattamento continua a fondarsi sulla medesima base giuridica dell'adempimento di un obbligo legale e dell'esecuzione di un compito di interesse pubblico ai sensi dell'art. 6, par. 1, lett. **c)** ed **e)** del GDPR. In tali casi il segnalante viene previamente informato delle modalità di registrazione o verbalizzazione della segnalazione.

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)?

Per quanto riguarda il principio di **minimizzazione dei dati**, l'impianto tecnico e organizzativo del trattamento appare coerente con quanto richiesto dall'art. 5, par. 1, lett. c) del GDPR. Il sistema adottato consente al segnalante di scegliere se fornire o meno le proprie generalità, senza alcuna forzatura: è quindi rispettato il principio secondo cui devono essere trattati solo i dati strettamente necessari. I campi dei moduli online distinguono tra informazioni obbligatorie (per consentire un'istruttoria concreta) e facoltative, e la piattaforma è strutturata in modo tale da **non obbligare il segnalante a identificarsi**, garantendo così un equilibrio tra esigenze istruttorie e protezione dei dati. Inoltre, qualora nella segnalazione vengano inseriti dati manifestamente non pertinenti, è prevista la cancellazione tempestiva degli stessi, come stabilito espressamente nella policy di retention del Comune. Il trattamento è quindi limitato ai soli dati rilevanti rispetto alla segnalazione, ed è gestito in modo proporzionato e non eccedente.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Sì, la procedura whistleblowing del Comune di Sant'Agello prevede misure idonee a garantire che i dati personali trattati siano **esatti, aggiornati e pertinenti**, in conformità all'art. 5, par. 1, lett. d) del GDPR. La qualità dei dati è assicurata, in primo luogo, dalla **modalità di raccolta diretta da parte del segnalante**, attraverso una piattaforma informatica che guida la compilazione del modulo e prevede campi strutturati con indicazioni chiare, aiutando l'utente a fornire informazioni circostanziate, coerenti e rilevanti.

In caso di **segnalazioni identificate tramite identificazione del segnalante**, i dati anagrafici vengono acquisiti in modo certo e automaticamente aggiornati, riducendo il rischio di errore o di incongruenza. Per le segnalazioni anonime o con generalità autodichiarate, l'accuratezza dei dati dipende dalle dichiarazioni del segnalante, ma la piattaforma prevede la possibilità, durante la fase istruttoria, di **richiedere chiarimenti o integrazioni**, tramite una chat asincrona sicura, che consente di arricchire o correggere i dati inizialmente trasmessi. Ogni interazione è tracciata, con data e ora, e rimane collegata alla segnalazione, favorendo la ricostruzione logica e coerente dei fatti.

Inoltre, il RPCT o il collaboratore incaricato ha il compito di verificare la **congruenza, completezza e attendibilità delle informazioni** durante l'esame preliminare. In caso di dati non aggiornati, incongruenti o palesemente non pertinenti, la segnalazione può essere considerata inammissibile oppure può essere sospesa in attesa di chiarimenti. Se vengono acquisiti **dati manifestamente inutili o eccedenti**, è previsto l'obbligo di cancellazione tempestiva, in conformità al principio di esattezza e minimizzazione.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

Per quanto riguarda il **periodo di conservazione dei dati**, come accennato, è stabilito in **cinque anni** dalla **comunicazione dell'esito finale della procedura di segnalazione**, come previsto dall'art. 14 del D.lgs. 24/2023 e come dichiarato anche nell'atto organizzativo adottato dal Comune. Tale periodo consente di gestire eventuali contenziosi successivi, segnalazioni di ritorsioni o verifiche da parte dell'ANAC, ed è coerente con i principi di proporzionalità e necessità previsti dalla normativa. I dati sono conservati in modo sicuro all'interno della piattaforma "Whistleblowing Intelligente", che impedisce modifiche o cancellazioni arbitrarie prima della scadenza del termine e garantisce il tracciamento di ogni operazione svolta. Decorso il periodo di conservazione, i dati vengono definitivamente cancellati secondo le modalità tecniche previste dal fornitore del servizio cloud.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati al trattamento dei dati personali nell'ambito della procedura di whistleblowing del Comune di Sant'Agnello sono informati **mediante un'apposita informativa privacy**, predisposta ai sensi dell'art. 13 del GDPR e pubblicata sul sito istituzionale del Comune, all'interno della sezione *Amministrazione Trasparente – Prevenzione della corruzione – Segnalazioni di illecito – whistleblower*. Tale informativa è anche **accessibile direttamente dalla piattaforma informatica "Whistleblowing Intelligente"**, sia nella home page di presentazione del servizio sia all'interno del modulo di segnalazione. Vengono chiaramente illustrate la finalità del trattamento, la base giuridica, la natura facoltativa o obbligatoria del conferimento, le misure di sicurezza adottate, i diritti dell'interessato e i riferimenti per contattare il titolare, il DPO e i responsabili del trattamento.

L'informativa è redatta in modo da garantire trasparenza anche nei confronti dei soggetti eventualmente menzionati nella segnalazione, nel rispetto delle limitazioni previste dalla normativa whistleblowing.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il **consenso dell'interessato** non è normalmente richiesto, in quanto il trattamento dei dati personali, anche appartenenti a categorie particolari o relativi a condanne penali, si basa sull'adempimento di un **obbligo legale** (art. 6, par. 1, lett. c) e art. 9, par. 2, lett. b) e g) del GDPR). Tuttavia, nel caso di **segnalazioni orali o vocali**, nonché nell'eventualità in cui sia necessario **disvelare l'identità del segnalante nell'ambito di un procedimento disciplinare**, viene richiesto il **consenso esplicito e inequivocabile**. La piattaforma consente di rilasciare tale consenso direttamente online, mediante un'interfaccia dedicata, che registra data, ora e scelta dell'utente. Una volta rilasciata, l'autorizzazione alla rivelazione dell'identità del segnalante produce effetti nell'ambito del procedimento disciplinare o giudiziario in cui è utilizzata, secondo quanto previsto dal D.lgs. 24/2023.

Valutazione : Accettabile

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

Per quanto riguarda l'esercizio dei diritti da parte degli interessati, il Comune di Sant'Agnello prevede che le richieste possano essere inviate ai recapiti istituzionali del Titolare o direttamente al **Responsabile della protezione dei dati (DPO)**, il cui indirizzo e-mail è indicato nell'informativa. Tuttavia, nel caso specifico delle segnalazioni whistleblowing, l'esercizio dei diritti di **accesso, portabilità, rettifica, cancellazione, limitazione e opposizione** può essere **legittimamente limitato o escluso**, ai sensi dell'art. 2-undecies del D.lgs. 196/2003, qualora il loro esercizio possa compromettere la **riservatezza dell'identità del segnalante** o pregiudicare le attività istruttorie connesse alla segnalazione. Ciò è coerente con quanto previsto anche dalla Direttiva (UE) 2019/1337 e dal D.lgs. 24/2023. Per i soggetti menzionati nella segnalazione (es. il segnalato), quindi, i diritti di accesso e rettifica non possono essere esercitati se da ciò può derivare un rischio effettivo e concreto per il segnalante.

Valutazione : Accettabile

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

Le richieste di rettifica o cancellazione possono essere esercitate dagli interessati contattando il Titolare o il DPO ai recapiti indicati nell'informativa. Tuttavia, nel caso specifico delle segnalazioni whistleblowing, l'esercizio dei diritti di **accesso, portabilità, rettifica, cancellazione, limitazione e opposizione** può essere **legittimamente limitato o escluso**, ai sensi dell'art. 2-undecies del D.lgs. 196/2003, qualora il loro esercizio possa compromettere la **riservatezza dell'identità del segnalante** o pregiudicare le attività istruttorie connesse alla segnalazione. Ciò è coerente con quanto previsto anche dalla Direttiva (UE) 2019/1337 e dal D.lgs. 24/2023. Per i soggetti menzionati nella segnalazione (es. il segnalato), quindi, i diritti di accesso e rettifica non possono essere esercitati se da ciò può derivare un rischio effettivo e concreto per il segnalante.

Valutazione : Accettabile

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

Gli interessati possono esercitare i diritti di limitazione del trattamento e di opposizione contattando il Titolare o il Responsabile della protezione dei dati ai recapiti indicati nell'informativa. Anche tali diritti possono essere limitati nei casi previsti dall'art. 2-undecies del D.lgs. 196/2003 qualora il loro esercizio possa compromettere la riservatezza dell'identità del segnalante o l'efficacia delle attività istruttorie.

Valutazione : Accettabile

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

Gli **obblighi dei responsabili del trattamento** sono definiti in modo formale mediante **nomina ai sensi dell'art. 28 del GDPR**. Il Comune di Sant'Agnello ha nominato **Tecnolink S.r.l.** responsabile del trattamento per la gestione della piattaforma whistleblowing, disciplinando l'ambito delle operazioni consentite, le misure di sicurezza, le responsabilità nei confronti del Titolare e i flussi di dati. Tecnolink, a sua volta, ha nominato **Interzen Consulting S.r.l.** quale **sub-responsabile**, per specifiche attività tecniche legate all'erogazione del servizio cloud. Entrambe le aziende operano nel rispetto di standard riconosciuti a livello europeo, in particolare attraverso l'**iscrizione allo STAR Registry della Cloud Security Alliance**, la **qualificazione presso il Marketplace ACN** (Agenzia per la Cybersicurezza Nazionale) e l'utilizzo di infrastruttura cloud **Microsoft Azure**, certificata secondo le principali normative di sicurezza informatica.

Valutazione : Accettabile

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

Non si configura alcun **trasferimento di dati al di fuori dell'Unione Europea**. La piattaforma opera su data center localizzati in **Europa occidentale (Paesi Bassi)** e **Europa settentrionale (Irlanda)**, come esplicitamente indicato nella documentazione tecnica. Pertanto, il trattamento dei dati resta sotto la giurisdizione europea, assicurando una **protezione equivalente a quella prevista dal GDPR** senza necessità di ulteriori garanzie contrattuali o clausole tipo.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

È applicata sia ai database che ai documenti, con chiavi criptate e gestione della decriptazione in fase di visualizzazione.

Valutazione : Accettabile

Anonimizzazione

La piattaforma consente l'invio di segnalazioni in forma anonima. Nei casi in cui il segnalante scelga di identificarsi, l'identità è protetta mediante misure tecniche e organizzative che ne impediscono la divulgazione a soggetti non autorizzati.

Valutazione : Accettabile

Controllo degli accessi logici

L'accesso alla piattaforma è regolato da login con credenziali univoche per RPCT e collaboratori; non è previsto accesso per altri soggetti.

Valutazione : Accettabile

Tracciabilità

Ogni accesso, modifica, apertura e rivelazione dell'identità è tracciato, registrato e notificato. Implementata nella piattaforma con registrazione completa delle attività.

Valutazione : Accettabile

Archiviazione

I dati sono conservati su Microsoft Azure in UE (West Europe e North Europe), con backup ciclici e politiche di retention di 5 anni.

Valutazione : Accettabile

Minimizzazione dei dati

Il modulo distingue tra campi obbligatori e facoltativi; i dati non rilevanti vengono cancellati.

Valutazione : Accettabile

Vulnerabilità

Utilizzo del sistema Nessus Essentials di Tenable per la scansione delle vulnerabilità.

Valutazione : Accettabile

Lotta contro il malware

Protezione antimalware implementata sui sistemi mediante soluzioni di sicurezza aggiornate e sistemi di monitoraggio delle minacce integrati nell'infrastruttura cloud.

Valutazione : Accettabile

Backup

Backup delle macchine virtuali ogni 4 ore, con retention di 15 giorni e archiviazione geografica.

Valutazione : Accettabile

Manutenzione

Previsto servizio di manutenzione evolutiva e normativa della piattaforma.

Valutazione : Accettabile

Contratto con il responsabile del trattamento

Tecnolink S.r.l. è formalmente nominata Responsabile ex art. 28 GDPR.

Valutazione : Accettabile

Sicurezza dei canali informatici

Protocollo HTTPS, autenticazione forte, crittografia dei canali di trasmissione.

Valutazione : Accettabile

Controllo degli accessi fisici

I dati sono conservati in data center sicuri (Azure), con misure fisiche certificate.

Valutazione : Accettabile

Sicurezza dell'hardware

Accesso tramite VPN, profilazione degli utenti, firewall PfSense.

Valutazione : Accettabile

Politica di tutela della privacy

Atto organizzativo comunale approvato con deliberazione n. 146/2023.

Valutazione : Accettabile

Gestione delle politiche di tutela della privacy

Attuata tramite nomina del DPO, informativa estesa, regolamento interno.

Valutazione : Accettabile

Gestione dei rischi

Il trattamento è soggetto a monitoraggio periodico dei rischi e a revisione delle misure tecniche e organizzative adottate.

Valutazione : Accettabile

Integrare la protezione della privacy nei progetti

Il sistema è progettato secondo i principi di privacy by design e by default ai sensi dell'art. 25 GDPR.

Valutazione : Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Sono previste procedure per la gestione degli incidenti di sicurezza e delle violazioni dei dati personali, in conformità agli artt. 33 e 34 del GDPR, con obbligo di segnalazione al Titolare e valutazione della notifica al Garante per la protezione dei dati personali.

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

Formalizzazione dei sub-responsabili (Interzen Consulting).

Valutazione : Accettabile

Vigilanza sulla protezione dei dati

Incarico al DPO e tracciamento delle attività del RPCT.

Valutazione : Accettabile

Rischi

Accesso illegittimo ai dati

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

Se il rischio di accesso illegittimo si dovesse concretizzare, le conseguenze per gli interessati – in particolare per i segnalanti – potrebbero essere molto gravi. Si includono: Perdita dell'anonimato del segnalante, con possibilità di ritorsioni personali o professionali. Compromissione della reputazione per le persone menzionate nelle segnalazioni. Danno psicologico, lavorativo, patrimoniale. Perdita di fiducia nel sistema pubblico, con effetto dissuasivo rispetto a future segnalazioni. Possibili conseguenze legali o disciplinari indebite in caso di informazioni divulgate o mal interpretate.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Attacco informatico al sistema (es. esfiltrazione, exploit, malware). Accesso non autorizzato da parte di personale interno (es. utenti amministrativi non autorizzati). Errata configurazione dei permessi di accesso o vulnerabilità di sistema. Violazione della segregazione dei ruoli tra RPCT e altri soggetti. Disattenzione umana (es. condivisione accidentale dell'identità del segnalante o errore di gestione dell'informazione). Fuga di dati tramite copia su supporti non sicuri o inoltro email.

Quali sono le fonti di rischio?

Infrastruttura informatica non correttamente aggiornata o protetta. Vulnerabilità nel sistema di autenticazione o nella crittografia. Comportamenti umani errati o dolosi. Accessi privilegiati

non gestiti secondo il principio del minimo privilegio. Eventuale inefficacia nel tracciamento delle attività o nella segregazione logica. Compromissione fisica dei dispositivi di amministrazione o server (anche se remoti).

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Gestione dei terzi che accedono ai dati, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati.

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

Importante, L'impatto potenziale in caso di accesso illegittimo è molto elevato, soprattutto per la particolare **vulnerabilità dei soggetti segnalanti**, tutelati espressamente dalla normativa nazionale ed europea. L'eventuale esposizione dell'identità di un whistleblower può compromettere in modo irreversibile la sua posizione personale e professionale. Tuttavia, la presenza di **misure tecniche e organizzative robuste** riduce significativamente il danno potenziale, seppure non lo annulla del tutto.

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

Limitata, Alla luce delle misure di mitigazione descritte, la probabilità che il rischio si verifichi è contenuta. Il sistema è protetto da più livelli di sicurezza informatica, segregazione delle identità e auditing continuo. Tuttavia, non può essere completamente esclusa l'eventualità di un attacco mirato o di errore umano residuo, motivo per cui il rischio resta da monitorare costantemente.

Valutazione : Accettabile

Commento di valutazione :

Alla luce delle misure tecniche e organizzative adottate, il rischio residuo può essere considerato accettabile in quanto la probabilità di accadimento risulta contenuta e proporzionata rispetto alle finalità del trattamento.

Rischi

Modifiche indesiderate dei dati

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

Se il rischio di modifiche indesiderate dei dati dovesse concretizzarsi, gli impatti sugli interessati potrebbero essere significativi, soprattutto in termini di alterazione della veridicità delle segnalazioni o dei documenti allegati. Un dato modificato impropriamente potrebbe: Compromettere l'integrità della segnalazione, falsando le risultanze istruttorie. Comportare conseguenze disciplinari o giudiziarie ingiustificate per soggetti menzionati. Inficiare la possibilità di dimostrare atti di ritorsione o abusi. Danneggiare la reputazione del segnalante o di terzi coinvolti. Determinare la perdita di fiducia nell'efficacia e nell'affidabilità del sistema di segnalazione.

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

Errore umano da parte di operatori autorizzati (es. editing non intenzionale del contenuto della segnalazione o dei metadati). Attacco informatico che sfrutta vulnerabilità della piattaforma per alterare i dati (es. injection, man-in-the-middle). Utilizzo improprio di privilegi di amministrazione da parte del fornitore tecnico o di soggetti interni all'organizzazione. Malfunzionamenti tecnici o bug del software (es. errata registrazione dei log o dei messaggi nella chat asincrona).

Quali sono le fonti di rischio?

Mancanza di versionamento dei dati o tracciamento delle modifiche su ogni campo/azione. Permessi eccessivamente ampi concessi a utenti interni o tecnici. Vulnerabilità software non corrette tempestivamente. Assenza di una procedura specifica di verifica delle modifiche effettuate post-registrazione.

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

Crittografia, Anonimizzazione, Archiviazione, Tracciabilità, Minimizzazione dei dati, Controllo degli accessi logici, Vulnerabilità, Lotta contro il malware, Backup, Manutenzione, Sicurezza dei canali informatici, Contratto con il responsabile del trattamento, Controllo degli accessi fisici, Sicurezza dell'hardware, Vigilanza sulla protezione dei dati, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione dei terzi che accedono ai dati.

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

Importante, La manipolazione, anche involontaria, dei dati contenuti in una segnalazione whistleblowing può generare conseguenze gravi, sia per l'interessato segnalato che per il segnalante. Può compromettere l'integrità probatoria e la tutela prevista dalla legge. Le misure tecniche implementate sono buone, ma il potenziale danno giuridico e reputazionale permane elevato in caso di incidente.

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

Limitata,

Grazie alla presenza di audit trail, backup frequenti, tracciabilità degli accessi e permessi strettamente regolati, la probabilità che si verifichino modifiche indesiderate è ridotta. Tuttavia, la possibilità di errore umano o vulnerabilità software non è del tutto eliminabile, per cui il rischio va tenuto sotto controllo.

Valutazione : Accettabile

Commento di valutazione :

Alla luce delle misure tecniche e organizzative adottate, il rischio residuo può essere considerato accettabile in quanto la probabilità di accadimento risulta contenuta e proporzionata rispetto alle finalità del trattamento.

Rischi

Perdita di dati

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

La perdita dei dati trattati nell'ambito della procedura di whistleblowing comporterebbe conseguenze molto rilevanti per gli interessati, a cominciare dai segnalanti. La scomparsa o cancellazione accidentale di una segnalazione può infatti: Compromettere in via definitiva la tutela del segnalante, rendendo impossibile la dimostrazione dell'avvenuta segnalazione e la protezione contro eventuali ritorsioni. Ostacolare o rendere impossibile l'avvio o il completamento di procedimenti interni o giudiziari fondati sulla segnalazione. Produrre danni reputazionali e istituzionali per l'amministrazione, con perdita di fiducia da parte di cittadini e dipendenti. Violare il diritto alla prova in sede disciplinare o contenziosa. Inficiare la possibilità di effettuare attività ispettive o di vigilanza da parte di ANAC o altre autorità pubbliche.

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

Malfunzionamenti del sistema informatico o errori nei processi di salvataggio (es. interruzioni di alimentazione, errori di sincronizzazione, crash di server). Attacchi informatici (es. ransomware, wiper malware) che cancellano o rendono inaccessibili i dati. Eliminazione accidentale da parte di un operatore autorizzato. Corruzione o danneggiamento fisico delle macchine virtuali o dei supporti cloud. Errori nei processi di backup o nei piani di disaster recovery.

Quali sono le fonti di rischio?

Mancata configurazione corretta dei backup automatici. Assenza di test periodici di ripristino (restore test). Interventi di manutenzione non tracciati o eseguiti in ambienti non isolati. Affidamento esclusivo a un unico data center senza replica geografica (non il caso in esame, ma rischio generale). Errori umani nella gestione del ciclo di vita delle segnalazioni (es. chiusura segnalazioni errata, cancellazione anticipata).

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

Anonimizzazione, Crittografia, Tracciabilità, Controllo degli accessi logici, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Backup, Manutenzione, Contratto con il responsabile del trattamento, Gestione dei terzi che accedono ai dati, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Integrare la protezione della privacy nei progetti, Gestione dei rischi, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati.

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

Importante, Sebbene il sistema sia strutturato per garantire un'elevata disponibilità dei dati, la perdita di segnalazioni whistleblowing può comportare **danni gravi e irreversibili**, soprattutto in termini di protezione del segnalante e di responsabilità dell'ente. L'impatto istituzionale e individuale è elevato. Le misure di mitigazione sono robuste, ma non possono annullare completamente la gravità del danno potenziale.

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

Trascurabile,

Grazie alla presenza di backup frequenti, disaster recovery cross-region, controllo degli accessi e segregazione dei dati, la probabilità effettiva che si verifichi una perdita irreversibile dei dati è estremamente bassa. Il sistema adotta tutte le contromisure previste dagli standard internazionali per garantire la disponibilità del dato.

Valutazione : Accettabile

Commento di valutazione :

Alla luce delle misure tecniche e organizzative adottate, il rischio residuo può essere considerato accettabile in quanto la probabilità di accadimento risulta contenuta e proporzionata rispetto alle finalità del trattamento.

Nome del DPO/RPD

Fabrizio Corona

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

All'esito della valutazione effettuata, si ritiene che il trattamento possa essere implementato in quanto le finalità perseguite risultano legittime, determinate e coerenti con gli obblighi normativi in materia di prevenzione della corruzione e tutela dei segnalanti previsti dal D.lgs. 24/2023 e dal Regolamento (UE) 2016/679. Le misure tecniche e organizzative adottate appaiono idonee a garantire un adeguato livello di sicurezza dei dati personali trattati, in

particolare sotto il profilo della riservatezza dell'identità del segnalante, della tracciabilità delle operazioni effettuate sulla piattaforma e della limitazione degli accessi ai soli soggetti autorizzati. Alla luce delle misure implementate e della valutazione dei rischi effettuata, il rischio residuo per i diritti e le libertà degli interessati può essere considerato accettabile e proporzionato rispetto alle finalità del trattamento.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non è stata effettuata una consultazione degli interessati nell'ambito della presente valutazione d'impatto. Tale scelta risulta giustificata dalla natura del trattamento, che riguarda la gestione di segnalazioni di illeciti e presuppone specifiche esigenze di riservatezza e protezione dell'identità del segnalante. Una consultazione preventiva degli interessati potrebbe infatti compromettere l'efficacia del sistema di segnalazione e pregiudicare le finalità di prevenzione e contrasto degli illeciti perseguite dalla normativa di riferimento. Il trattamento è pertanto disciplinato mediante specifiche misure organizzative e tecniche volte a garantire la tutela dei diritti e delle libertà degli interessati, in conformità al Regolamento (UE) 2016/679 e al D.lgs. 24/2023.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento in considerazione riguarda la gestione delle segnalazioni di illeciti o irregolarità, disciplinate dalla procedura di whistleblowing adottata dal Comune di Sant'Agnello. La procedura si inserisce nell'ambito della normativa nazionale e comunitaria che tutela i segnalanti, ovvero le persone che, venute a conoscenza di comportamenti illeciti o irregolari nell'ambito del loro lavoro, decidono di segnalarli alle autorità competenti. La piattaforma utilizzata per raccogliere queste segnalazioni è denominata "**Whistleblowing Intelligente**", un sistema basato su un servizio SaaS (Software as a Service) che consente di raccogliere segnalazioni sia in forma anonima che identificata. Le segnalazioni possono essere inviate tramite una piattaforma informatica, ma anche mediante segnalazioni vocali o orali su appuntamento, a seconda della preferenza del segnalante.

Il trattamento può riguardare dati personali relativi ai segnalanti, ai soggetti segnalati e ad eventuali altri soggetti coinvolti nella segnalazione. Le categorie di dati trattati possono comprendere dati identificativi e di contatto, dati relativi al rapporto di lavoro o di collaborazione con l'ente e, ove strettamente necessari ai fini della gestione della segnalazione, informazioni relative a presunte condotte illecite.

Le finalità del trattamento dei dati raccolti riguardano principalmente la gestione delle segnalazioni, la verifica dell'eventuale violazione delle normative, e l'attuazione di misure

protettive per tutelare il segnalante da eventuali ritorsioni. La piattaforma assicura la riservatezza del segnalante e dei dati, rispettando gli obblighi previsti dal **D.lgs. 24/2023** (che recepisce la Direttiva (UE) 2019/1937) in tema di protezione dei whistleblower. I risultati attesi da questa procedura sono la corretta gestione e trattazione delle segnalazioni, la protezione dei diritti dei segnalanti e la promozione della legalità all'interno dell'amministrazione comunale. L'obiettivo è garantire che ogni segnalazione venga trattata con riservatezza, e che venga presa una decisione appropriata in merito all'eventuale azione correttiva da intraprendere. L'uso della piattaforma garantisce che le segnalazioni vengano gestite in modo sicuro e tracciato, rispettando la privacy del segnalante e delle persone coinvolte.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità connesse al trattamento sono distribuite tra diversi soggetti coinvolti nel processo.

Il **Titolare del trattamento** è il **Comune di Sant'Agnello**, che è l'entità giuridica principale che gestisce e definisce la politica del trattamento dei dati personali, prendendo decisioni finali sul trattamento e garantendo la conformità alla normativa.

All'interno del Comune, l'**RPCT** (Responsabile della prevenzione della corruzione e della trasparenza) ha il compito di gestire il processo operativo delle segnalazioni e garantire che vengano seguite tutte le procedure interne per rispondere alle segnalazioni ricevute.

Il **Responsabile della protezione dei dati (DPO)**, nominato dal Comune, è incaricato di supervisionare il rispetto della normativa sulla protezione dei dati personali e fornire supporto nella gestione delle problematiche relative alla privacy.

Inoltre, la piattaforma "Whistleblowing Intelligente" è gestita dalla società **Tecnolink S.r.l.**, che funge da **Responsabile del trattamento** ai sensi dell'art. 28 del GDPR. Tecnolink è incaricata della gestione tecnica della piattaforma e dei dati personali relativi alle segnalazioni, ma opera sotto le istruzioni del Comune di Sant'Agnello.

Ci sono standard applicabili al trattamento?

Per quanto riguarda gli **standard applicabili al trattamento**, il sistema adottato dal Comune di Sant'Agnello segue gli standard stabiliti dal **GDPR (Regolamento (UE) n. 2016/679)**, che garantisce la protezione dei dati personali. In particolare, il trattamento dei dati deve rispettare il principio di **privacy by design and by default**, che implica che le misure di protezione dei dati siano integrate fin dalla progettazione della piattaforma. Inoltre, vengono rispettati gli standard di **cybersecurity**, con la piattaforma registrata nel **Cloud Marketplace dell'Autorità per la Cybersicurezza Nazionale (ACN)**, che ne certifica la sicurezza e l'affidabilità. La piattaforma implementa misure tecniche come la **crittografia dei dati**, la **segretezza dei dati identificativi del segnalante**, e l'**accesso limitato** ai dati da parte solo di soggetti autorizzati, in conformità con le Linee guida ANAC e le normative sulla protezione dei dati. Il sistema assicura anche l'**audit trail**, ovvero la **tracciabilità degli accessi e delle operazioni effettuate sui dati**.

In relazione agli standard applicabili al trattamento, è opportuno segnalare che, oltre alla conformità al **Regolamento (UE) 2016/679 (GDPR)** e al **D.lgs. 24/2023**, il Comune di Sant'Agnello ha formalmente adottato un **Atto Organizzativo di Attuazione della Disciplina del Whistleblowing**, approvato con **deliberazione di Giunta Comunale n. 146 del 12/12/2023**.

Tale documento rappresenta uno **standard interno vincolante**, che definisce puntualmente ruoli, responsabilità, modalità operative e misure di sicurezza da applicare al trattamento dei dati personali nell'ambito della gestione delle segnalazioni. L'atto si configura come parte integrante del sistema di compliance dell'ente, in attuazione delle **Linee guida ANAC n. 469/2021**, e garantisce un presidio organizzativo strutturato e trasparente in materia di whistleblowing, rafforzando l'affidabilità del trattamento sotto il profilo sia giuridico che procedurale.

Valutazione : Accettabile

Commento di valutazione :

Sulla base delle informazioni disponibili, le misure tecniche e organizzative implementate risultano adeguate e proporzionate rispetto ai rischi individuati, rendendo il trattamento accettabile sotto il profilo della protezione dei dati personali.

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati personali trattati possono essere suddivisi in più categorie, a seconda della modalità di segnalazione e del contenuto stesso della segnalazione. Vengono trattati **dati identificativi del segnalante** (qualora non anonimo), **dati delle persone coinvolte o menzionate nella segnalazione**, **dati relativi ai fatti segnalati**, nonché eventuali **categorie particolari di dati ai sensi dell'art. 9 del GDPR** (ad esempio dati relativi a opinioni politiche, stato di salute, convinzioni religiose o appartenenza sindacale) e **dati relativi a condanne penali o reati** (art. 10 GDPR), se pertinenti. In aggiunta, dati relativi alla registrazione della voce del segnalante, ove la segnalazione avvenga tramite canale vocale.

Il periodo di conservazione previsto è pari a **5 anni dalla comunicazione dell'esito finale della segnalazione**, come disposto dall'art. 14 del D.lgs. 24/2023 e come riportato nell'atto organizzativo interno. I dati non pertinenti o manifestamente inutili vengono cancellati tempestivamente. I **destinatari dei dati** possono essere, laddove necessario, l'Autorità Nazionale Anticorruzione (ANAC), l'Autorità Giudiziaria, la Corte dei conti o l'Ufficio Provvedimenti Disciplinari, a seconda della natura e dell'esito della segnalazione. I **sogetti autorizzati all'accesso** ai dati sono esclusivamente il **Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT)**, nonché gli eventuali collaboratori da lui formalmente designati e istruiti. Nessun altro soggetto può accedere ai dati, né è consentita la diffusione degli stessi. In caso di accesso ai dati identificativi del segnalante, la piattaforma registra la motivazione e notifica l'avvenuto accesso al segnalante stesso.

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

Il ciclo di vita dei dati segue un processo articolato, tracciato dalla piattaforma **Whistleblowing Intelligente**, strutturato come segue:

- **Raccolta dei dati:** avviene tramite piattaforma web sicura, accesso tramite piattaforma web sicura che consente l'invio della segnalazione sia in forma identificata sia anonima. Il segnalante può allegare documenti, registrazioni vocali o inserire riferimenti a terzi. In alternativa, la segnalazione può essere acquisita oralmente (telefono o incontro diretto).
- **Registrazione e protocollazione:** il sistema assegna automaticamente un ID univoco e registra data e ora della segnalazione, impedendo modifiche o cancellazioni.
- **Presa in carico:** il RPCT riceve una notifica della segnalazione ed è l'unico soggetto abilitato a leggerla entro 7 giorni. In caso di necessità, può affidarne la gestione a un collaboratore interno.
- **Valutazione preliminare:** vengono esaminati i presupposti formali per la ricevibilità (contenuto circostanziato, riferibilità all'Ente, pertinenza).
- **Istruttoria:** si sviluppano eventuali richieste di chiarimento al segnalante, consultazioni documentali e raccolta di ulteriori elementi. Tutte le attività sono tracciate nella piattaforma.
- **Chiusura della segnalazione:** al termine dell'istruttoria (entro 90 giorni), si redige un verbale interno nella piattaforma, che può condurre all'archiviazione o alla trasmissione ad ANAC, autorità giudiziaria o Corte dei conti.
- **Archiviazione:** i dati restano disponibili nella piattaforma per un periodo massimo di 5 anni. Anche dopo la chiusura, la chat asincrona tra segnalante e RPCT resta attiva per eventuali aggiornamenti o segnalazioni di ritorsioni.
- **Cancellazione:** decorso il termine, i dati vengono eliminati in conformità alla policy di retention.

Quali sono le risorse di supporto ai dati?

Le risorse di supporto al trattamento comprendono sia componenti tecniche che organizzative. I dati sono ospitati all'interno della piattaforma **Whistleblowing Intelligente**, basata su infrastruttura cloud **Microsoft Azure**, localizzata in data center situati nell'Unione Europea (Paesi Bassi e Irlanda). La protezione dei dati è garantita tramite crittografia dei database e dei documenti, autenticazione forte degli utenti autorizzati, segregazione delle informazioni riservate, firewall e sistemi antivirus. I sistemi operativi impiegati sono virtualizzati e accessibili unicamente tramite VPN. Il back-up delle macchine virtuali avviene ogni 4 ore, con retention di 15 giorni e disaster recovery cross-region attivo. Il software è conforme agli standard di sicurezza definiti dal **Cloud Marketplace dell'ACN**, ed è registrato anche presso lo **STAR Registry della Cloud Security Alliance**.

Le risorse umane coinvolte nel trattamento sono i soggetti formalmente incaricati dal Titolare, in particolare il **RPCT**, i collaboratori autorizzati, e il **DPO** in funzione di vigilanza. I supporti fisici (es. cartacei) sono esclusi dalla procedura, salvo segnalazioni eccezionali ricevute con mezzi tradizionali, che vengono protocollate in registri riservati e trattate con le stesse garanzie di riservatezza e integrità previste per il canale informatico.

Valutazione : Accettabile

Commento di valutazione :

Alla luce delle misure tecniche e organizzative implementate, il trattamento risulta adeguatamente presidiato e i rischi individuati possono ritenersi accettabili rispetto alle finalità perseguite.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento effettuato dal Comune di Sant'Agnello nell'ambito della procedura whistleblowing sono pienamente **specifici, espliciti e legittimi**. Il trattamento dei dati personali ha come finalità principale quella di consentire la ricezione, la gestione e l'istruttoria delle segnalazioni di illeciti o irregolarità, nel rispetto della normativa nazionale (D.lgs. 24/2023), del diritto europeo (Direttiva (UE) 2019/1937) nonché con le Linee guida ANAC in materia di gestione delle segnalazioni di illeciti e con le misure organizzative adottate dall'Ente nell'ambito del proprio sistema di prevenzione della corruzione e della trasparenza.. Si tratta di una finalità chiaramente definita e collegata a un obbligo giuridico, quale la tutela dell'interesse pubblico, l'integrità dell'amministrazione e la protezione delle persone che segnalano violazioni di legge. Inoltre, le finalità sono esplicitate nel testo dell'atto organizzativo adottato dall'ente (delibera di Giunta n. 146/2023), nonché nell'informativa fornita al momento della segnalazione, e sono accessibili anche tramite i canali ufficiali dell'amministrazione.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La legittimità delle finalità deriva dalla necessità di adempiere a obblighi legali specifici previsti dalla normativa anticorruzione e in materia di protezione dei whistleblower. In particolare, la base giuridica che rende lecito il trattamento è rappresentata, ai sensi dell'art. 6, par. 1 lett. **c)** del GDPR, dall'adempimento di un **obbligo legale** al quale è soggetto il Titolare, ovvero il Comune di Sant'Agnello, in quanto amministrazione pubblica tenuta ad attivare canali di segnalazione sicuri ed efficaci. Per il trattamento di eventuali **categorie particolari di dati** (art. 9 GDPR), si applicano le lettere **b)** e **g)** dello stesso articolo, poiché il trattamento è necessario per adempiere a obblighi nel campo del diritto del lavoro e per motivi di interesse pubblico rilevante. Per le segnalazioni effettuate oralmente tramite canali vocali, il trattamento continua a fondarsi sulla medesima base giuridica dell'adempimento di un obbligo legale e dell'esecuzione di un compito di interesse pubblico ai sensi dell'art. 6, par. 1, lett. **c)** ed **e)** del GDPR. In tali casi il segnalante viene previamente informato delle modalità di registrazione o verbalizzazione della segnalazione.

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)?

Per quanto riguarda il principio di **minimizzazione dei dati**, l'impianto tecnico e organizzativo del trattamento appare coerente con quanto richiesto dall'art. 5, par. 1, lett. c) del GDPR. Il sistema adottato consente al segnalante di scegliere se fornire o meno le proprie generalità, senza alcuna forzatura: è quindi rispettato il principio secondo cui devono essere trattati solo i dati strettamente necessari. I campi dei moduli online distinguono tra informazioni obbligatorie (per consentire un'istruttoria concreta) e facoltative, e la piattaforma è strutturata in modo tale da **non obbligare il segnalante a identificarsi**, garantendo così un equilibrio tra esigenze istruttorie e protezione dei dati. Inoltre, qualora nella segnalazione vengano inseriti dati manifestamente non pertinenti, è prevista la cancellazione tempestiva degli stessi, come stabilito espressamente nella policy di retention del Comune. Il trattamento è quindi limitato ai soli dati rilevanti rispetto alla segnalazione, ed è gestito in modo proporzionato e non eccedente.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Sì, la procedura whistleblowing del Comune di Sant'Agello prevede misure idonee a garantire che i dati personali trattati siano **esatti, aggiornati e pertinenti**, in conformità all'art. 5, par. 1, lett. d) del GDPR. La qualità dei dati è assicurata, in primo luogo, dalla **modalità di raccolta diretta da parte del segnalante**, attraverso una piattaforma informatica che guida la compilazione del modulo e prevede campi strutturati con indicazioni chiare, aiutando l'utente a fornire informazioni circostanziate, coerenti e rilevanti.

In caso di **segnalazioni identificate tramite identificazione del segnalante**, i dati anagrafici vengono acquisiti in modo certo e automaticamente aggiornati, riducendo il rischio di errore o di incongruenza. Per le segnalazioni anonime o con generalità autodichiarate, l'accuratezza dei dati dipende dalle dichiarazioni del segnalante, ma la piattaforma prevede la possibilità, durante la fase istruttoria, di **richiedere chiarimenti o integrazioni**, tramite una chat asincrona sicura, che consente di arricchire o correggere i dati inizialmente trasmessi. Ogni interazione è tracciata, con data e ora, e rimane collegata alla segnalazione, favorendo la ricostruzione logica e coerente dei fatti.

Inoltre, il RPCT o il collaboratore incaricato ha il compito di verificare la **congruenza, completezza e attendibilità delle informazioni** durante l'esame preliminare. In caso di dati non aggiornati, incongruenti o palesemente non pertinenti, la segnalazione può essere considerata inammissibile oppure può essere sospesa in attesa di chiarimenti. Se vengono acquisiti **dati manifestamente inutili o eccedenti**, è previsto l'obbligo di cancellazione tempestiva, in conformità al principio di esattezza e minimizzazione.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

Per quanto riguarda il **periodo di conservazione dei dati**, come accennato, è stabilito in **cinque anni** dalla **comunicazione dell'esito finale della procedura di segnalazione**, come previsto dall'art. 14 del D.lgs. 24/2023 e come dichiarato anche nell'atto organizzativo adottato dal Comune. Tale periodo consente di gestire eventuali contenziosi successivi, segnalazioni di ritorsioni o verifiche da parte dell'ANAC, ed è coerente con i principi di proporzionalità e necessità previsti dalla normativa. I dati sono conservati in modo sicuro all'interno della piattaforma "Whistleblowing Intelligente", che impedisce modifiche o cancellazioni arbitrarie prima della scadenza del termine e garantisce il tracciamento di ogni operazione svolta. Decorso il periodo di conservazione, i dati vengono definitivamente cancellati secondo le modalità tecniche previste dal fornitore del servizio cloud.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati al trattamento dei dati personali nell'ambito della procedura di whistleblowing del Comune di Sant'Agnello sono informati **mediante un'apposita informativa privacy**, predisposta ai sensi dell'art. 13 del GDPR e pubblicata sul sito istituzionale del Comune, all'interno della sezione *Amministrazione Trasparente – Prevenzione della corruzione – Segnalazioni di illecito – whistleblower*. Tale informativa è anche **accessibile direttamente dalla piattaforma informatica "Whistleblowing Intelligente"**, sia nella home page di presentazione del servizio sia all'interno del modulo di segnalazione. Vengono chiaramente illustrate la finalità del trattamento, la base giuridica, la natura facoltativa o obbligatoria del conferimento, le misure di sicurezza adottate, i diritti dell'interessato e i riferimenti per contattare il titolare, il DPO e i responsabili del trattamento.

L'informativa è redatta in modo da garantire trasparenza anche nei confronti dei soggetti eventualmente menzionati nella segnalazione, nel rispetto delle limitazioni previste dalla normativa whistleblowing.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il **consenso dell'interessato** non è normalmente richiesto, in quanto il trattamento dei dati personali, anche appartenenti a categorie particolari o relativi a condanne penali, si basa sull'adempimento di un **obbligo legale** (art. 6, par. 1, lett. c) e art. 9, par. 2, lett. b) e g) del GDPR). Tuttavia, nel caso di **segnalazioni orali o vocali**, nonché nell'eventualità in cui sia necessario **disvelare l'identità del segnalante nell'ambito di un procedimento disciplinare**, viene richiesto il **consenso esplicito e inequivocabile**. La piattaforma consente di rilasciare tale consenso direttamente online, mediante un'interfaccia dedicata, che registra data, ora e scelta dell'utente. Una volta rilasciata, l'autorizzazione alla rivelazione dell'identità del segnalante produce effetti nell'ambito del procedimento disciplinare o giudiziario in cui è utilizzata, secondo quanto previsto dal D.lgs. 24/2023.

Valutazione : Accettabile

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

Per quanto riguarda l'esercizio dei diritti da parte degli interessati, il Comune di Sant'Agnello prevede che le richieste possano essere inviate ai recapiti istituzionali del Titolare o direttamente al **Responsabile della protezione dei dati (DPO)**, il cui indirizzo e-mail è indicato nell'informativa. Tuttavia, nel caso specifico delle segnalazioni whistleblowing, l'esercizio dei diritti di **accesso, portabilità, rettifica, cancellazione, limitazione e opposizione** può essere **legittimamente limitato o escluso**, ai sensi dell'art. 2-undecies del D.lgs. 196/2003, qualora il loro esercizio possa compromettere la **riservatezza dell'identità del segnalante** o pregiudicare le attività istruttorie connesse alla segnalazione. Ciò è coerente con quanto previsto anche dalla Direttiva (UE) 2019/1937 e dal D.lgs. 24/2023. Per i soggetti menzionati nella segnalazione (es. il segnalato), quindi, i diritti di accesso e rettifica non possono essere esercitati se da ciò può derivare un rischio effettivo e concreto per il segnalante.

Valutazione : Accettabile

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

Le richieste di rettifica o cancellazione possono essere esercitate dagli interessati contattando il Titolare o il DPO ai recapiti indicati nell'informativa. Tuttavia, nel caso specifico delle segnalazioni whistleblowing, l'esercizio dei diritti di **accesso, portabilità, rettifica, cancellazione, limitazione e opposizione** può essere **legittimamente limitato o escluso**, ai sensi dell'art. 2-undecies del D.lgs. 196/2003, qualora il loro esercizio possa compromettere la **riservatezza dell'identità del segnalante** o pregiudicare le attività istruttorie connesse alla segnalazione. Ciò è coerente con quanto previsto anche dalla Direttiva (UE) 2019/1937 e dal D.lgs. 24/2023. Per i soggetti menzionati nella segnalazione (es. il segnalato), quindi, i diritti di accesso e rettifica non possono essere esercitati se da ciò può derivare un rischio effettivo e concreto per il segnalante.

Valutazione : Accettabile

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

Gli interessati possono esercitare i diritti di limitazione del trattamento e di opposizione contattando il Titolare o il Responsabile della protezione dei dati ai recapiti indicati nell'informativa. Anche tali diritti possono essere limitati nei casi previsti dall'art. 2-undecies del D.lgs. 196/2003 qualora il loro esercizio possa compromettere la riservatezza dell'identità del segnalante o l'efficacia delle attività istruttorie.

Valutazione : Accettabile

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

Gli **obblighi dei responsabili del trattamento** sono definiti in modo formale mediante **nomina ai sensi dell'art. 28 del GDPR**. Il Comune di Sant'Agnello ha nominato **Tecnolink S.r.l.** responsabile del trattamento per la gestione della piattaforma whistleblowing, disciplinando l'ambito delle operazioni consentite, le misure di sicurezza, le responsabilità nei confronti del Titolare e i flussi di dati. Tecnolink, a sua volta, ha nominato **Interzen Consulting S.r.l.** quale **sub-responsabile**, per specifiche attività tecniche legate all'erogazione del servizio cloud. Entrambe le aziende operano nel rispetto di standard riconosciuti a livello europeo, in particolare attraverso l'**iscrizione allo STAR Registry della Cloud Security Alliance**, la **qualificazione presso il Marketplace ACN** (Agenzia per la Cybersicurezza Nazionale) e l'utilizzo di infrastruttura cloud **Microsoft Azure**, certificata secondo le principali normative di sicurezza informatica.

Valutazione : Accettabile

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

Non si configura alcun **trasferimento di dati al di fuori dell'Unione Europea**. La piattaforma opera su data center localizzati in **Europa occidentale (Paesi Bassi)** e **Europa settentrionale (Irlanda)**, come esplicitamente indicato nella documentazione tecnica. Pertanto, il trattamento dei dati resta sotto la giurisdizione europea, assicurando una **protezione equivalente a quella prevista dal GDPR** senza necessità di ulteriori garanzie contrattuali o clausole tipo.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

È applicata sia ai database che ai documenti, con chiavi criptate e gestione della decriptazione in fase di visualizzazione.

Valutazione : Accettabile

Anonimizzazione

La piattaforma consente l'invio di segnalazioni in forma anonima. Nei casi in cui il segnalante scelga di identificarsi, l'identità è protetta mediante misure tecniche e organizzative che ne impediscono la divulgazione a soggetti non autorizzati.

Valutazione : Accettabile

Controllo degli accessi logici

L'accesso alla piattaforma è regolato da login con credenziali univoche per RPCT e collaboratori; non è previsto accesso per altri soggetti.

Valutazione : Accettabile

Tracciabilità

Ogni accesso, modifica, apertura e rivelazione dell'identità è tracciato, registrato e notificato. Implementata nella piattaforma con registrazione completa delle attività.

Valutazione : Accettabile

Archiviazione

I dati sono conservati su Microsoft Azure in UE (West Europe e North Europe), con backup ciclici e politiche di retention di 5 anni.

Valutazione : Accettabile

Minimizzazione dei dati

Il modulo distingue tra campi obbligatori e facoltativi; i dati non rilevanti vengono cancellati.

Valutazione : Accettabile

Vulnerabilità

Utilizzo del sistema Nessus Essentials di Tenable per la scansione delle vulnerabilità.

Valutazione : Accettabile

Lotta contro il malware

Protezione antimalware implementata sui sistemi mediante soluzioni di sicurezza aggiornate e sistemi di monitoraggio delle minacce integrati nell'infrastruttura cloud.

Valutazione : Accettabile

Backup

Backup delle macchine virtuali ogni 4 ore, con retention di 15 giorni e archiviazione geografica.

Valutazione : Accettabile

Manutenzione

Previsto servizio di manutenzione evolutiva e normativa della piattaforma.

Valutazione : Accettabile

Contratto con il responsabile del trattamento

Tecnolink S.r.l. è formalmente nominata Responsabile ex art. 28 GDPR.

Valutazione : Accettabile

Sicurezza dei canali informatici

Protocollo HTTPS, autenticazione forte, crittografia dei canali di trasmissione.

Valutazione : Accettabile

Controllo degli accessi fisici

I dati sono conservati in data center sicuri (Azure), con misure fisiche certificate.

Valutazione : Accettabile

Sicurezza dell'hardware

Accesso tramite VPN, profilazione degli utenti, firewall PfSense.

Valutazione : Accettabile

Politica di tutela della privacy

Atto organizzativo comunale approvato con deliberazione n. 146/2023.

Valutazione : Accettabile

Gestione delle politiche di tutela della privacy

Attuata tramite nomina del DPO, informativa estesa, regolamento interno.

Valutazione : Accettabile

Gestione dei rischi

Il trattamento è soggetto a monitoraggio periodico dei rischi e a revisione delle misure tecniche e organizzative adottate.

Valutazione : Accettabile

Integrare la protezione della privacy nei progetti

Il sistema è progettato secondo i principi di privacy by design e by default ai sensi dell'art. 25 GDPR.

Valutazione : Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Sono previste procedure per la gestione degli incidenti di sicurezza e delle violazioni dei dati personali, in conformità agli artt. 33 e 34 del GDPR, con obbligo di segnalazione al Titolare e valutazione della notifica al Garante per la protezione dei dati personali.

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

Formalizzazione dei sub-responsabili (Interzen Consulting).

Valutazione : Accettabile

Vigilanza sulla protezione dei dati

Incarico al DPO e tracciamento delle attività del RPCT.

Valutazione : Accettabile

Rischi

Accesso illegittimo ai dati

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

Se il rischio di accesso illegittimo si dovesse concretizzare, le conseguenze per gli interessati – in particolare per i segnalanti – potrebbero essere molto gravi. Si includono: Perdita dell'anonimato del segnalante, con possibilità di ritorsioni personali o professionali. Compromissione della reputazione per le persone menzionate nelle segnalazioni. Danno psicologico, lavorativo, patrimoniale. Perdita di fiducia nel sistema pubblico, con effetto dissuasivo rispetto a future segnalazioni. Possibili conseguenze legali o disciplinari indebite in caso di informazioni divulgate o mal interpretate.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Attacco informatico al sistema (es. esfiltrazione, exploit, malware). Accesso non autorizzato da parte di personale interno (es. utenti amministrativi non autorizzati). Errata configurazione dei permessi di accesso o vulnerabilità di sistema. Violazione della segregazione dei ruoli tra RPCT e altri soggetti. Disattenzione umana (es. condivisione accidentale dell'identità del segnalante o errore di gestione dell'informazione). Fuga di dati tramite copia su supporti non sicuri o inoltro email.

Quali sono le fonti di rischio?

Infrastruttura informatica non correttamente aggiornata o protetta. Vulnerabilità nel sistema di autenticazione o nella crittografia. Comportamenti umani errati o dolosi. Accessi privilegiati non gestiti secondo il principio del minimo privilegio. Eventuale inefficacia nel tracciamento delle attività o nella segregazione logica. Compromissione fisica dei dispositivi di amministrazione o server (anche se remoti).

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Gestione dei terzi che accedono ai dati, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati

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

Importante, L'impatto potenziale in caso di accesso illegittimo è molto elevato, soprattutto per la particolare **vulnerabilità dei soggetti segnalanti**, tutelati espressamente dalla normativa nazionale ed europea. L'eventuale esposizione dell'identità di un whistleblower può compromettere in modo irreversibile la sua posizione personale e professionale. Tuttavia, la presenza di **misure tecniche e organizzative robuste** riduce significativamente il danno potenziale, seppure non lo annulla del tutto.

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

Limitata, Alla luce delle misure di mitigazione descritte, la probabilità che il rischio si verifichi è contenuta. Il sistema è protetto da più livelli di sicurezza informatica, segregazione delle identità e auditing continuo. Tuttavia, non può essere completamente esclusa l'eventualità di un attacco mirato o di errore umano residuo, motivo per cui il rischio resta da monitorare costantemente.

Valutazione : Accettabile

Commento di valutazione :

Alla luce delle misure tecniche e organizzative adottate, il rischio residuo può essere considerato accettabile in quanto la probabilità di accadimento risulta contenuta e proporzionata rispetto alle finalità del trattamento.

Rischi

Modifiche indesiderate dei dati

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

Se il rischio di modifiche indesiderate dei dati dovesse concretizzarsi, gli impatti sugli interessati potrebbero essere significativi, soprattutto in termini di alterazione della veridicità delle segnalazioni o dei documenti allegati. Un dato modificato impropriamente potrebbe: Compromettere l'integrità della segnalazione, falsando le risultanze istruttorie. Comportare conseguenze disciplinari o giudiziarie ingiustificate per soggetti menzionati. Inficiare la possibilità di dimostrare atti di ritorsione o abusi. Danneggiare la reputazione del segnalante o di terzi coinvolti. Determinare la perdita di fiducia nell'efficacia e nell'affidabilità del sistema di segnalazione.

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

Errore umano da parte di operatori autorizzati (es. editing non intenzionale del contenuto della segnalazione o dei metadati). Attacco informatico che sfrutta vulnerabilità della piattaforma per alterare i dati (es. injection, man-in-the-middle). Utilizzo improprio di privilegi di amministrazione da parte del fornitore tecnico o di soggetti interni all'organizzazione. Malfunzionamenti tecnici o bug del software (es. errata registrazione dei log o dei messaggi nella chat asincrona).

Quali sono le fonti di rischio?

Mancanza di versionamento dei dati o tracciamento delle modifiche su ogni campo/azione. Permessi eccessivamente ampi concessi a utenti interni o tecnici. Vulnerabilità software non corrette tempestivamente. Assenza di una procedura specifica di verifica delle modifiche effettuate post-registrazione.

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

Crittografia, Anonimizzazione, Archiviazione, Tracciabilità, Minimizzazione dei dati, Controllo degli accessi logici, Vulnerabilità, Lotta contro il malware, Backup, Manutenzione, Sicurezza dei canali informatici, Contratto con il responsabile del trattamento, Controllo degli accessi fisici, Sicurezza dell'hardware, Vigilanza sulla protezione dei dati, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione dei terzi che accedono ai dati

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

Importante, La manipolazione, anche involontaria, dei dati contenuti in una segnalazione whistleblowing può generare conseguenze gravi, sia per l'interessato segnalato che per il segnalante. Può compromettere l'integrità probatoria e la tutela prevista dalla legge. Le misure tecniche implementate sono buone, ma il potenziale danno giuridico e reputazionale permane elevato in caso di incidente.

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

Limitata,

Grazie alla presenza di audit trail, backup frequenti, tracciabilità degli accessi e permessi strettamente regolati, la probabilità che si verifichino modifiche indesiderate è ridotta. Tuttavia, la possibilità di errore umano o vulnerabilità software non è del tutto eliminabile, per cui il rischio va tenuto sotto controllo.

Valutazione : Accettabile

Commento di valutazione :

Alla luce delle misure tecniche e organizzative adottate, il rischio residuo può essere considerato accettabile in quanto la probabilità di accadimento risulta contenuta e proporzionata rispetto alle finalità del trattamento.

Rischi

Perdita di dati

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

La perdita dei dati trattati nell'ambito della procedura di whistleblowing comporterebbe conseguenze molto rilevanti per gli interessati, a cominciare dai segnalanti. La scomparsa o cancellazione accidentale di una segnalazione può infatti: Compromettere in via definitiva la tutela del segnalante, rendendo impossibile la dimostrazione dell'avvenuta segnalazione e la protezione contro eventuali ritorsioni. Ostacolare o rendere impossibile l'avvio o il completamento di procedimenti interni o giudiziari fondati sulla segnalazione. Produrre danni reputazionali e istituzionali per l'amministrazione, con perdita di fiducia da parte di cittadini e dipendenti. Violare il diritto alla prova in sede disciplinare o contenziosa. Inficiare la possibilità di effettuare attività ispettive o di vigilanza da parte di ANAC o altre autorità pubbliche.

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

Malfunzionamenti del sistema informatico o errori nei processi di salvataggio (es. interruzioni di alimentazione, errori di sincronizzazione, crash di server). Attacchi informatici (es. ransomware, wiper malware) che cancellano o rendono inaccessibili i dati. Eliminazione accidentale da parte di un operatore autorizzato. Corruzione o danneggiamento fisico delle macchine virtuali o dei supporti cloud. Errori nei processi di backup o nei piani di disaster recovery.

Quali sono le fonti di rischio?

Mancata configurazione corretta dei backup automatici. Assenza di test periodici di ripristino (restore test). Interventi di manutenzione non tracciati o eseguiti in ambienti non isolati. Affidamento esclusivo a un unico data center senza replica geografica (non il caso in esame, ma rischio generale). Errori umani nella gestione del ciclo di vita delle segnalazioni (es. chiusura segnalazioni errata, cancellazione anticipata).

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

Anonimizzazione, Crittografia, Tracciabilità, Controllo degli accessi logici, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Backup, Manutenzione, Contratto con il responsabile del trattamento, Gestione dei terzi che accedono ai dati, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Integrare la protezione della privacy nei progetti, Gestione dei rischi, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati

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

Importante, Sebbene il sistema sia strutturato per garantire un'elevata disponibilità dei dati, la perdita di segnalazioni whistleblowing può comportare **danni gravi e irreversibili**, soprattutto in termini di protezione del segnalante e di responsabilità dell'ente. L'impatto istituzionale e individuale è elevato. Le misure di mitigazione sono robuste, ma non possono annullare completamente la gravità del danno potenziale.

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

Trascurabile,

Grazie alla presenza di backup frequenti, disaster recovery cross-region, controllo degli accessi e segregazione dei dati, la probabilità effettiva che si verifichi una perdita irreversibile dei dati è estremamente bassa. Il sistema adotta tutte le contromisure previste dagli standard internazionali per garantire la disponibilità del dato.

Valutazione : Accettabile

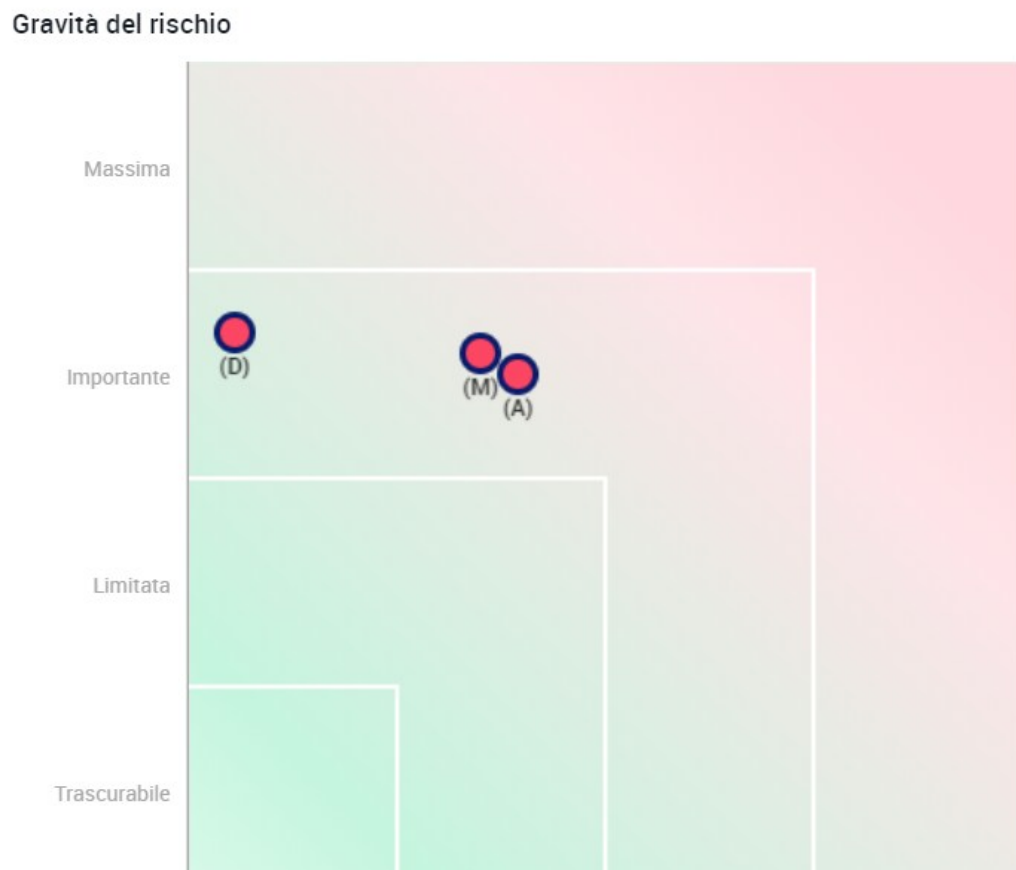
Commento di valutazione :

Alla luce delle misure tecniche e organizzative adottate, il rischio residuo può essere considerato accettabile in quanto la probabilità di accadimento risulta contenuta e

proporzionata rispetto alle finalità del trattamento.

























Rischi

Panoramica dei rischi



Panoramica

Principi fondamentali

Finalità		
Basi legali		
Adeguatezza dei dati		
Esattezza dei dati		
Periodo di conservazione		
Informativa		
Raccolta del consenso		
Diritto di accesso e diritto alla portabilità dei dati		
Diritto di rettifica e diritto di cancellazione		
Diritto di limitazione e diritto di opposizione		
Responsabili del trattamento		
Trasferimenti di dati		

Misure esistenti o pianificate

		Crittografia
		Anonimizzazione
		Controllo degli accessi logici
		Tracciabilità
		Archiviazione
		Minimizzazione dei dati
		Vulnerabilità
		Lotta contro il malware
		Backup
		Manutenzione
		Contratto con il responsabile del trattamento
		Sicurezza dei canali informatici
		Controllo degli accessi fisici
		Sicurezza dell'hardware
		Politica di tutela della privacy
		Gestione delle politiche di tutela della privacy
		Gestione dei rischi
		Integrare la protezione della privacy nei progetti
		Gestire gli incidenti di sicurezza e le violazioni dei dati personali
		Gestione dei terzi che accedono ai dati
		Vigilanza sulla protezione dei

Impatti potenziali

Se il rischio di accesso il...
Se il rischio di modifiche ..
La perdita dei dati trattat...

Minaccia

Attacco informatico al sist..
Errore umano da parte di op
Malfunzionamenti del siste

Fonti

Infrastruttura informatica ..
Mancanza di versionament
Mancata configurazione co

Misure

Crittografia
Anonimizzazione
Controllo degli accessi log.
Tracciabilità
Archiviazione
Minimizzazione dei dati
Vulnerabilità
Lotta contro il malware
Backup
Manutenzione
Contratto con il responsabi.
Sicurezza dei canali inform
Gestione dei terzi che acce.
Controllo degli accessi fis..
Sicurezza dell'hardware
Politica di tutela della pr..
Gestione delle politiche di..
Gestione dei rischi
Integrare la protezione del..
Gestire gli incidenti di si..
Vigilanza sulla protezione .

Accesso illegittimo ai dati

Gravità : Importante

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Importante

Probabilità : Limitata

Perdita di dati

Gravità : Importante

Probabilità : Trascurabile

