

Valutazione d'impatto (DPIA) del sistema di ricevimento e gestione delle segnalazioni interne WHISTLEBLOWING

Ai sensi dell'art. 35 REGOLAMENTO(UE) 2016/679

Titolare del trattamento	Comune di Masera		
Responsabile della Protezione dei Dati personali (DPO/RPD):	Labor Service S.r.l. Dott.ssa Angela Emanuele		
Autori	• Dott. Pierpaolo Nicolosi RPCT • Dott.ssa Angela Emanuele Responsabile della Protezione dei Dati personali		
Data di emissione	29/03/2024	Versione	00

Sommario

1. Riferimenti normativi.....	3
2. Doverosità di svolgere la DPIA.....	4
3. Contesto	4
3.1. Panoramica del trattamento.....	4
3.2. Dati, processi e risorse di supporto	5
3.3. Proporzionalità e necessità.....	6
3.4. Misure a tutela dei diritti degli interessati.....	7
4. Rischi.....	8
4.1. Misure esistenti o pianificate.....	8
4.2. Accesso illegittimo ai dati.....	9
4.3. Modifiche indesiderate dei dati	10
4.4. Perdita di dati	10
4.5. Panoramica dei rischi	12
4.6. Valutazione del rischio.....	13
5. Parere del DPO e degli interessati.....	13
6. Conclusioni	14

1. Riferimenti normativi

La valutazione d'impatto (o, altrimenti detta, DPIA – *Data Protection Impact Assessment*) è una procedura prevista dall'articolo 35 del Regolamento (UE) 2016/679 (GDPR) che il titolare deve svolgere allorché intraprenda un'attività di trattamento particolarmente delicata. Lo scopo è quello di verificare l'impatto del trattamento sui diritti e le libertà degli interessati, valutandone, da una parte, la necessità e la proporzionalità rispetto al fine da perseguire, dall'altra, l'idoneità delle misure di sicurezza approntate per annullare o almeno limitare i rischi di incidenti. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Si riporta qui di seguito il testo integrale della citata norma, dove sono specificatamente indicate le condizioni al ricorrere delle quali è doverosa la valutazione d'impatto.

1. 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 previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorché svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
 - a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un **trattamento automatizzato**, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
 - b) il **trattamento, su larga scala, di categorie particolari di dati personali** di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
 - c) la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico**.
4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.
6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.
7. **La valutazione contiene** almeno:
 - a) una **descrizione sistematica dei trattamenti previsti e delle finalità del trattamento**, compreso, ove applicabile, l'**interesse legittimo** perseguito dal titolare del trattamento;

- b) una valutazione della **necessità e proporzionalità** dei trattamenti in relazione alle finalità;
- c) una **valutazione dei rischi per i diritti e le libertà** degli interessati di cui al paragrafo 1; e
- d) le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.
11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

2. Doverosità di svolgere la DPIA

I soggetti del settore pubblico sono tenuta a norma del D.Lgs. 24/2023 ad adottare un modello di ricevimento e gestione delle segnalazioni interne di whistleblowing che comporta il trattamento da parte dell'RPCT di informazioni su illeciti (dati giudiziari) commessi all'interno dell'ente rivelati da segnalanti la cui identità deve rimanere riservata e conoscibile solo dalle persone autorizzate.

Tali segnalazioni comportano un trattamento di dati personali che può rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento.

Pertanto, risulta obbligatoria la redazione del presente documento ai sensi dell'art. 35 GDPR anche alla luce dell'espressa previsione contenuta nell'art. 13, comma 6, del D.Lgs. 24/2023.

3. Contesto

3.1. Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento dei dati riguarda le persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica, di cui siano venute a conoscenza nel contesto lavorativo (c.d. Whistleblowing) ai sensi della L. 179/2017 e del D.Lgs. 24/2023. Inoltre, il trattamento dei dati riguarda anche i soggetti a cui è attribuito l'illecito e gli eventuali altri soggetti coinvolti come i facilitatori, persone del medesimo contesto lavorativo legate al segnalante da uno

stabile legame affettivo o di parentela entro il quarto grado e i colleghi di lavoro del segnalante che hanno con detta persona un rapporto abituale e corrente.

Chi segnala fornisce informazioni che possono portare all'indagine, all'accertamento e al perseguimento dei casi di violazione delle norme, rafforzando in tal modo i principi di trasparenza e responsabilità delle istituzioni democratiche.

Garantire la protezione dei soggetti che si espongono con segnalazioni, denunce o con l'istituto della divulgazione pubblica, contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per la stessa amministrazione e, di riflesso, per l'interesse pubblico collettivo.

Tale protezione è estesa anche a soggetti diversi da chi segnala, come il facilitatore o le persone menzionate nella segnalazione, a conferma dell'intenzione, del legislatore europeo e italiano, di creare condizioni per rendere l'istituto in questione un importante presidio per la legalità, per la concorrenza e per garantire il buon andamento e l'imparzialità delle pubbliche amministrazioni.

Il Comune, per adempiere a quanto richiesto dalla normativa, istituisce un canale di segnalazione interno sia scritto che orale conforme a quanto indicato nelle LLGG Anac del 12 luglio 2023.

Quali sono le responsabilità connesse al trattamento?

Il Comune di Masera è Titolare del trattamento ed ha individuato nella figura del Responsabile della prevenzione della corruzione e della trasparenza (c.d. RPCT) il soggetto competente a gestire le segnalazioni pervenute attraverso il canale di segnalazione interno.

L'RPCT, incarico ricoperto negli enti locali dal segretario comunale, sarà autorizzato al trattamento dei dati con apposita lettera redatta ai sensi dell'art. 29 GDPR.

Per tale trattamento non sono stati individuati dei Responsabili del trattamento ex art. 28 GDPR.

Ci sono standard applicabili al trattamento?

La Procedura adottata dal Comune è conforme a quanto richiesto dal D.Lgs. 24/2023 e dalle LLGG Anac del 12 luglio 2023.

3.2. Dati, processi e risorse di supporto

Quali sono i dati trattati?

- Dati identificativi: dati anagrafici e di contatto del segnalante (qualora non si proceda con segnalazione anonima) e dati identificativi del segnalato e di altri soggetti citati nella segnalazione;
- Categorie particolari di dati: dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati;
- Dati relativi a condanne penali e reati: dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Sono destinatari dei dati raccolti a seguito della segnalazione, se del caso, l'Autorità Giudiziaria, la Corte dei conti e l'ANAC.

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

Le segnalazioni possono pervenire, ed essere quindi raccolte, tramite la modulistica messa a disposizione sul sito internet istituzionale nella sezione "Prevenzione della Corruzione" ed inviata per mezzo posta con indicazione di Riservata all'RPCT.

Per quanto riguarda le segnalazioni attraverso il canale di segnalazione scritto predisposto dal Comune il ciclo di vita del trattamento è il seguente:

- 1) Download della modulistica in formato editabile;
- 2) Compilazione dei due moduli (oggetto della segnalazione e identità del segnalante);
- 3) Invio della segnalazione a mezzo posta con indicazione di Riservata all'RPCT;
- 4) Smistamento della posta e consegna all'RPCT che invierà apposita ricevuta di ricezione al segnalante;

- 5) Analisi della segnalazione (analisi preliminare e successiva istruttoria) e gestione da parte dell'RPCT attraverso indagini interne, anche attraverso audizioni, o richieste con adozione di provvedimenti conseguenti;
- 6) Chiusura di una segnalazione e invio riscontro al segnalante e conservazione fino al termine di 5 anni dalla comunicazione di chiusura;
- 7) Cancellazione sicura dei dati al termine del periodo di conservazione.

Quali sono le risorse di supporto ai dati?

Archivio riservato all'RPCT dotato di serratura.

3.3. Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati riguardanti le persone che segnalano una violazione, le persone a cui la violazione è attribuita e gli altri soggetti eventualmente coinvolti è previsto da norme di legge che ne stabiliscono la finalità e la legittimità. In particolare, la L. 179/2017 e il D.lgs. 24/2023 sono volte a favorire il processo di segnalazione. Infatti, garantire la protezione dei soggetti che si espongono con segnalazioni, denunce o con l'istituto della divulgazione pubblica, contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per la stessa amministrazione e, di riflesso, per l'interesse pubblico collettivo.

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento dei dati personali degli interessati è individuabile nell'obbligo di legge (art. 6, lett. c) GDPR) previsto in capo al Titolare del trattamento, consistente nel dover prevenire rischi e situazioni pregiudizievoli per l'interesse pubblico (art. 6, lett. e) GDPR) con danno, anche soltanto d'immagine, per l'Ente e nel dover individuare strumenti di tutela nei confronti dei lavoratori che denuncino reati o irregolarità di cui siano venuti a conoscenza nell'ambito delle proprie attività lavorative (L. 179/2017 e D.lgs. 24/2023). Inoltre, la base giuridica che legittima la comunicazione dei dati personali del segnalante al segnalato nell'ambito del procedimento disciplinare, qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, è il consenso espresso della persona segnalante alla rivelazione della sua identità (art. 6, lett. a) GDPR).

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

La modulistica predisposta dall'Ente richiede solo i dati identificativi necessari al fine di attivare le tutele previste dalla normativa.

In particolare, sono richiesti i seguenti dati al segnalante:

- Nome e cognome;
- Recapito telefonico e indirizzo di posta elettronica;
- Qualifica e mansione svolta all'epoca dei fatti segnalati;
- Qualifica svolta al momento della segnalazione se diversa da quella precedente.

In riferimento al soggetto segnalato, sono richiesti i seguenti dati:

- Nome e cognome;
- Qualifica e mansione svolta all'epoca dei fatti segnalati;
- Fatto imputato.

Infine, nella modulistica è richiesto di indicare i dati anagrafici di eventuali soggetti che possono riferire sul fatto.

I dati sono esatti e aggiornati?

L'aggiornamento dei dati è a cura dell'RPCT che dà seguito ad una richiesta di rettifica o integrazione dei dati personali da parte del segnalante o degli altri soggetti secondo la procedura di gestione delle richieste di esercizio dei diritti privacy adottata dal Comune.

Qual è il periodo di conservazione dei dati?

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario alla gestione delle stesse e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione (art. 14 D.Lgs. 24/2023).

3.4. Misure a tutela dei diritti degli interessati

Come sono informati del trattamento degli interessati?

Il Comune di Masera mette a disposizione dei soggetti interessati (segnalante, segnalato, altri soggetti coinvolti) apposita informativa privacy resa ai sensi dell'art. 13 GDPR nella sezione privacy e nella sezione dedicata alle segnalazioni di whistleblowing sul proprio sito internet istituzionale. In tale ultima sezione verranno, inoltre, resi disponibili la procedura adottata dall'ente, la modulistica necessaria per l'invio delle segnalazioni e le ulteriori indicazioni sulla gestione delle segnalazioni di whistleblowing.

Ove applicabile: come si ottiene il consenso degli interessati?

Per il trattamento dei dati relativi alla procedura di whistleblowing non è necessario raccogliere un consenso dell'interessato in quanto il trattamento ha quale base giuridica l'adempimento di un obbligo di legge a cui è soggetto il Titolare del trattamento.

Il D.Lgs. 24/2023 disciplina però due ipotesi in cui è necessario raccogliere il consenso del segnalante quale soggetto interessato:

- 1) La prima ipotesi ricorre laddove nell'ambito di un procedimento disciplinare avviato nei confronti del presunto autore della condotta segnalata, l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare. In tal caso, oltre al previo consenso del segnalante da raccogliere per iscritto è necessario anche comunicare, sempre previamente, in forma scritta a quest'ultimo le motivazioni che conducono al disvelamento della sua identità.
- 2) La seconda ipotesi ricorre, invece, nel caso in cui nelle procedure di segnalazione interna ed esterna la rivelazione dell'identità del segnalante sia indispensabile anche ai fini della difesa della persona coinvolta. Anche in questo caso per disvelare l'identità del segnalante è necessario acquisire previamente sia il consenso espresso dello stesso che notificare allo stesso, in forma scritta, le motivazioni alla base della necessità di disvelare la sua identità.

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

Il Comune di Masera ha adottato una procedura di gestione delle richieste di esercizio dei diritti in materia di privacy e ha previsto la pubblicazione sul proprio sito istituzione nella sezione Privacy di un modulo con cui il soggetto interessato può esercitare i suoi diritti.

Nel dettaglio, il segnalante può esercitare il diritto accesso ai propri dati rivolgendosi direttamente all'RPCT mentre i soggetti segnalati o altri soggetti coinvolti nella segnalazione (es. testimoni) possono esercitare, ai sensi dell'art. 2-undecies, lett. f) e parag. 3) del D.Lgs. 196/2003, tale diritto per il tramite del Garante Privacy con la modalità di cui all'art. 160 del D.Lgs. 196/2003.

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

Il Comune di Masera ha adottato una procedura di gestione delle richieste di esercizio dei diritti in materia di privacy e ha previsto la pubblicazione sul proprio sito istituzione nella sezione Privacy di un modulo con cui il soggetto interessato può esercitare i suoi diritti. Nel dettaglio, il segnalante può esercitare il diritto di rettifica e cancellazione rivolgendosi direttamente all'RPCT mentre i soggetti segnalati o altri soggetti coinvolti nella segnalazione (es. testimoni) possono esercitare, ai sensi dell'art. 2-undecies, lett. f) e parag. 3) del D.Lgs. 196/2003, tali diritti per il tramite del Garante Privacy con la modalità di cui all'art. 160 del D.Lgs. 196/2003.

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

Il Comune di Masera ha adottato una procedura di gestione delle richieste di esercizio dei diritti in materia di privacy e ha previsto la pubblicazione sul proprio sito istituzione nella sezione Privacy di un modulo con cui il soggetto interessato può esercitare i suoi diritti. Nel dettaglio, il segnalante può esercitare i diritti di limitazione e opposizione ai propri dati rivolgendosi direttamente all'RPCT mentre i soggetti segnalati o altri soggetti coinvolti nella segnalazione (es. testimoni) possono esercitare, ai sensi dell'art. 2-undecies, lett. f) e parag. 3) del D.Lgs. 196/2003, tali diritti per il tramite del Garante Privacy con la modalità di cui all'art. 160 del D.Lgs. 196/2003.

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

Non sono previsti Responsabili del trattamento per questa specifica attività di trattamento.

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

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

4. Rischi

4.1. Misure esistenti o pianificate

Partizionamento

La modulistica predisposta dal Comune prevede un apposito modulo in cui riportare i dati identificativi del segnalante separato da altro modulo in cui si riporta la segnalazione di illecito e il suo autore. La divisione della modulistica consente di tenere separate l'identità del segnalante dal fatto segnalato così da rendere anonima la segnalazione anche qualora questa per fini istruttoria debba essere portata a conoscenza di altri soggetti.

La modulistica scaricabile in formato editabile consente di procedere alla compilazione in modalità digitale senza la necessità di eventuale compilazione a mano che permetterebbe, indirettamente, l'identificabilità del segnalante.

Archiviazione

Le segnalazioni sono archiviate a cura dell'RPCT in distinti archivi dotati di serratura ad accesso esclusivo al fine di non rendere vana la misura di partizionamento dell'oggetto della segnalazione dall'identità del segnalante.

L'RPCT attraverso protocollazione separata e riservata della segnalazione sarà sempre in grado di associare una segnalazione al segnalante.

Sicurezza dei documenti cartacei

I documenti cartacei relativi alle segnalazioni di whistleblowing sono conservati in archivi dotati di serratura accessibili al solo RPCT.

Nel caso in cui la segnalazione dovesse pervenire erroneamente mediante casella e-mail ordinaria e/o posta elettronica certificata, il dipendente autorizzato ad accedere al protocollo che leggerà erroneamente la segnalazione, dovrà stampare la segnalazione e tutti gli eventuali allegati ritirando immediatamente le copie cartacee dalla stampante al fine di non far accedere persone terze e inserire tutto quanto in una busta chiusa apponendo all'esterno l'indicazione "SEGNALAZIONE ILLECITI - RISERVATA AL RPCT" e contestualmente eliminare la e-mail ordinaria e/o posta elettronica certificata ricevuta; successivamente dovrà trasmettere la busta al RPCT, entro sette giorni dal suo ricevimento, ricordandogli di fornire riscontro sulla trasmissione della segnalazione al soggetto segnalante conservando sotto chiave la busta o comunque in un luogo accessibile soltanto al dipendente, fino alla sua consegna al RPCT. Sono vietate copie della documentazione relativa alle segnalazioni di whistleblowing.

Minimizzazione dei dati

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati o distrutti senza indugio da parte dell'RPCT.

Controllo degli accessi fisici

Gli archivi predisposti per la conservazione delle segnalazioni di whistleblowing ad opera dell'RPCT dovranno essere collocati in luoghi accessibili solo a questo e dotati di serratura.

Protezione contro fonti di rischio non umane

Gli archivi contenenti le segnalazioni di whistleblowing sono collocati in luoghi riservati all'interno dell'edificio comunale presso cui sono state adottate misure di sicurezza dell'ambiente quali misure antincendio.

Politica di tutela della privacy

Il Comune di Masera ha nominato un DPO esterno ai sensi dell'art. 37 GDPR che svolge i compiti stabiliti dall'art. 39 GDPR sulla base di un contratto di servizi.

Inoltre, il personale dipendente del Comune di Masera svolge periodicamente una formazione in materia di protezione dei dati personali comprensiva anche dei rischi informatici ed è stato istruito rispetto al corretto trattamento dei dati.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Il Comune ha adottato una procedura di gestione delle violazioni dei dati personali (c.d. Data Breach).

Gestione del personale

Il personale autorizzato all'accesso ai dati delle segnalazioni di whistleblowing è stato appositamente nominato, istruito e formato sia in materia di protezione dei dati personali che in materia di whistleblowing. Inoltre, nella Procedura elaborata dal Comune si stabilisce che al cessare dell'incarico di RPCT, il vecchio gestore trasferisce tutti i dati e le informazioni al nuovo gestore, cancellando eventuali copie e garantendo il rispetto della riservatezza anche al cessare dell'incarico.

4.2. Accesso illegittimo ai dati

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

Danno per la reputazione

Discriminazione

Perdita di controllo dei dati

Altri svantaggi economici e sociali

Impossibilità di esercitare diritti, servizi o opportunità

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Errore umano

Furto dei supporti fisici di archiviazione

Quali sono le fonti di rischio?

Persona interna o esterna al Comune

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Partizionamento

Archiviazione

Sicurezza dei documenti cartacei

Minimizzazione dei dati

Controllo degli accessi fisici

Politica di tutela della privacy

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

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

Massima.

L'impatto per il segnalante è sicuramente alto in quanto lo stesso potrebbe essere discriminato e ricevere ritorsione nel proprio contesto lavorativo a seguito della segnalazione effettuata se questa viene resa nota o accessibile a persone non autorizzate.

Anche il soggetto segnalato potrebbe avere degli impatti alti derivanti dalla diffusione del proprio nominativo quale potenziale autore di reato a maggior ragione qualora la segnalazione risulti poi non fondata.

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

Limitata.

Le misure implementate riducono la probabilità che l'evento si verifichi.

4.3. Modifiche indesiderate dei dati

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

Danno per la reputazione.

Discriminazione.

Altri svantaggi economici e sociali.

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

Errore umano.

Quali sono le fonti di rischio?

Persona interna o esterna al Comune.

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

Sicurezza dei documenti cartacei

Controllo degli accessi fisici

Politica di tutela della privacy

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Gestione del personale

Archiviazione

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

Importante.

L'impatto per il segnalante è sicuramente importante in quanto i dati potrebbero non essere esatti e dunque determinare delle problematiche di comunicazione con l'RPCT oppure determinare degli errori nell'azione di verifica dell'RPCT conseguenti alla segnalazione.

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

Limitata.

Le misure implementate riducono la probabilità che l'evento si verifichi.

4.4. Perdita di dati

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

Impossibilità di esercitare diritti, servizi o opportunità.
Altri svantaggi economici e sociali.

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

Errore umano
Furto dei supporti fisici di archiviazione e registrazione
Evento esterno quale incendio

Quali sono le fonti di rischio?

Persona interna o esterna al Comune
Evento esterno quale incendio

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

Archiviazione
Sicurezza dei documenti cartacei
Controllo degli accessi fisici
Protezione contro fonti di rischio non umane
Politica di tutela della privacy
Gestire gli incidenti di sicurezza e le violazioni dei dati personali
Gestione del personale

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

Importante.
L'impatto per il segnalante è sicuramente importante in quanto lo stesso non potrebbe più esercitare i diritti a lui spettanti o la tutela prevista dalla normativa oltre che determinare l'impossibilità di procedere con le verifiche conseguenti alla segnalazione.

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

Limitata.
Le misure implementate riducono la probabilità che l'evento si verifichi.

Impatti potenziali

Danno per la reputazione
Discriminazione
Perdita di controllo dei dati
Altri svantaggi economici e
Impossibilità di esercitare...

Minaccia

Errore umano
Furto dei supporti fisici d...
Evento esterno quale incen...

Fonti

Persona interna o esterna a...
Evento esterno quale incen...

Misure

Partizionamento
Archiviazione
Sicurezza dei documenti ca...
Minimizzazione dei dati
Controllo degli accessi fis...
Politica di tutela della pr...
Gestire gli incidenti di si...
Gestione del personale
Protezione contro fonti di ..

Accesso illegittimo ai dati

Gravità : Massima

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Importante

Probabilità : Limitata

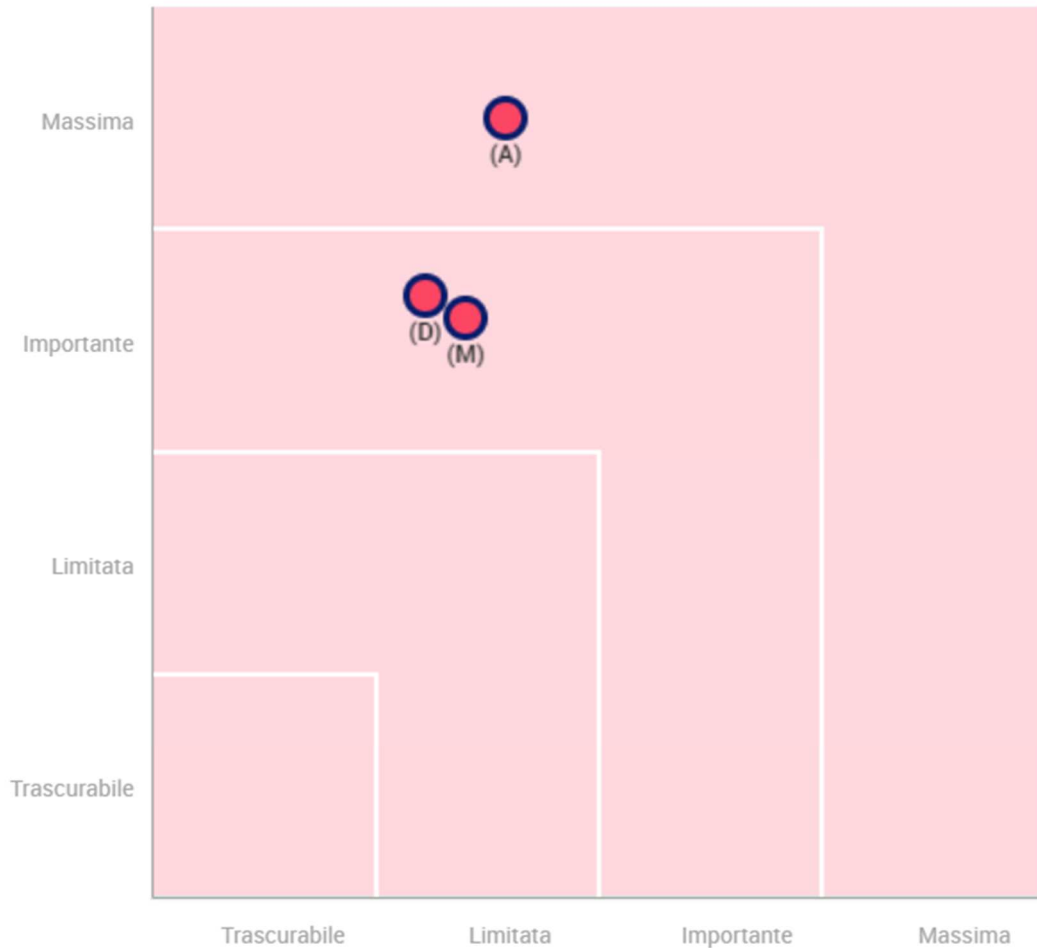
Perdita di dati

Gravità : Importante

Probabilità : Limitata

4.6. Valutazione del rischio

Gravità del rischio



- **Misure pianificate o esistenti**
- **Con le misure correttive implementate**
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Probabilità del rischio

02/11/23

5. Parere del DPO e degli interessati

Parere del DPO:

Le misure di sicurezza previste consentono di operare ai sensi della normativa rispettando la riservatezza del segnalante, del segnalato e degli eventuali soggetti terzi. Il trattamento essendo previsto per legge può essere svolto nelle modalità analizzate.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Il trattamento oggetto di valutazione potenzialmente coinvolge un numero non definito e una tipologia di interessati vari e, pertanto, è impossibile richiederne un parere.

In ogni caso, come richiesto dal D.Lgs. 24/2023 la Procedura di segnalazioni illeciti (whistleblowing) è stata inviata alle organizzazioni sindacali per eventuali osservazioni in merito.

6. Conclusioni

Dopo aver valutato nel dettaglio quanto richiesto dal par. 7 dell'art. 35 GDPR, il Comune può concludere che il trattamento dei dati relativo alle ricezione e gestione delle segnalazioni di whistleblowing analizzato risulta:

- 1) **Proporzionato** alla finalità previste da normativa: le misure poste a protezione dei dati personali dei soggetti coinvolti nel procedimento di whistleblowing consente di ritenere il trattamento proporzionato rispetto ai diritti e alle libertà dei soggetti interessati.
- 2) È **necessario**, in quanto tale finalità è prevista da legge nel rispetto di adeguate misure di sicurezza poste a protezione dei dati personali degli interessati.