



DPIA

Data Protection Impact Assessment – DPIA

ai sensi dell'art. 35 del Regolamento UE 2016/679

**Trattamento dati personali per la segnalazione degli illeciti
(Whistleblowing)**

Indice

Indice	2
1 Gestione documento	7
2 Contesto	8
2.1 Ambito di applicazione	8
2.1.1 Trattamento oggetto della valutazione	8
2.1.2 Obiettivi e metodologia applicata	8
2.1.3 Responsabilità legate al trattamento	10
2.1.4 Normative e standard applicabili al trattamento	12
2.1.4.1 Valutazione	15
2.2.1 Tipologie di dati trattati	15
2.2.2 Ciclo di vita del trattamento dei dati	16
2.2.3 Risorse di supporto ai dati	17
2.2.3.1 Valutazione	17
3 Principi Fondamentali	18
3.1 Finalità, proporzionalità, necessità	18
3.1.1 Finalità del trattamento	18
3.1.2 Basi giuridiche del trattamento	19
3.1.3 Minimizzazione dei dati trattati	19
3.1.4 L'accuratezza e l'attualità dei dati	20
3.1.5 Durata della conservazione dei dati	20
3.1.6 Valutazione	21
3.2 Controlli per proteggere i diritti personali dei soggetti interessati	21
	2

3.2.1	Le modalità di informativa ai soggetti interessati	21
3.2.2	Raccolta del consenso dei soggetti interessati	22
3.2.3	Modalità di esercizio del diritto di accesso ai dati da parte dei soggetti interessati	22
3.2.4	Modalità di esercizio del diritto alla rettifica e alla cancellazione dei dati da parte dei soggetti interessati	23
3.2.5	Modalità di esercizio del diritto di limitazione e opposizione dei dati da parte dei soggetti interessati	23
3.2.6	Obblighi dei responsabili del trattamento	24
3.2.7	Protezione dei dati nel caso di trasferimento di dati fuori dall'Unione Europea	25
3.2.8	Valutazione	25
4	Rischi	25
4.1	Controlli esistenti o pianificati	25
4.1.1	Crittografia	25
4.1.1.1	Valutazione	26
4.1.2	Anonimizzazione	26
4.1.2.1	Valutazione	27
4.1.3	Partizionamento dei dati	27
4.1.3.1	Valutazione	27
4.1.4	Controllo degli accessi logici	28
4.1.4.1	Valutazione	28
4.1.5	Tracciabilità	28
4.1.5.1	Valutazione	29
4.1.6	Archiviazione	29
4.1.6.1	Valutazione	30
4.1.7	Sicurezza dei documenti cartacei	30
		3

4.1.7.1	Valutazione	30
4.1.8	Minimizzazione dei dati	30
4.1.8.1	Valutazione	31
4.1.9	Vulnerabilità	31
4.1.9.1	Valutazione	32
4.1.9	Lotta contro il malware	32
4.1.10.1	Valutazione	32
4.1.11	Gestione postazioni	33
4.1.11.1	Valutazione	33
4.1.12	Sicurezza dei siti web	33
4.1.12.1	Valutazione	34
4.1.13	Backup	34
4.1.13.1	Valutazione	34
4.1.14	Manutenzione	34
4.1.14.1	Valutazione	35
4.1.15	Contratto con il responsabile del trattamento	35
4.1.15.1	Valutazione	36
4.1.16	Sicurezza dei canali informatici	36
4.1.16.1	Valutazione	36
4.1.17	Controllo degli accessi fisici	37
4.1.17.1	Valutazione	37
4.1.18	Sicurezza dell'hardware	37
4.1.18.1	Valutazione	38
4.1.19	Protezione contro fonti di rischio non umane	38

4.1.19.1 Valutazione	38
4.1.20 Politica di tutela della privacy	38
4.1.20.1 Valutazione	39
4.1.21 Gestione delle politiche di tutela della privacy	39
4.1.21.1 Valutazione	40
4.1.22 Gestione dei rischi	40
4.1.22.1 Valutazione	41
4.1.23 Integrare la protezione della privacy nei progetti	41
4.1.23.1 Valutazione	41
4.1.24 Gestire gli incidenti di sicurezza e le violazioni dei dati personali	42
4.1.24.1 Valutazione	42
4.1.25 Gestione del personale	42
4.1.25.1 Valutazione	43
4.1.26 Gestione dei terzi che accedono ai dati	43
4.1.26.1 Valutazione	44
4.1.27.1 Valutazione	44
4.2 Rischio di accesso illegittimo ai dati	45
4.2.1 Impatti potenziali sui soggetti interessati se il rischio si dovesse concretizzare	45
4.2.2 Principali minacce che potrebbero concretizzare il rischio	47
4.2.3 Fonti di rischio	48
4.2.4 Misure individuate che contribuiscono a mitigare il rischio	48
4.2.5 Gravità del rischio, riguardo i potenziali impatti e i controlli pianificati	51
4.2.6 Probabilità del rischio, riguardo alle minacce, alle fonti di rischio e alle misure pianificate	51
4.2.7 Valutazione complessiva	51
	5

4.2.7.1	Valutazione	51
4.3	Rischio di modifiche indesiderate dei dati	52
4.3.1	Impatti potenziali sui soggetti interessati se il rischio si dovesse concretizzare	52
4.3.3	Fonti di rischio	55
4.3.4	Misure individuate che contribuiscono a mitigare il rischio	55
4.3.5	Gravità del rischio riguardo ai potenziali impatti e alle misure pianificate	57
4.3.6	Probabilità del rischio riguardo minacce, fonti di rischio e controlli pianificati	58
4.3.7	Valutazione complessiva	58
4.3.7.1	Valutazione	58
4.4	Rischio di perdita di dati	59
4.4.1	Impatto sui soggetti interessati se il rischio dovesse realizzarsi	59
4.4.3	Fonti di rischio	61
4.4.4	Misure fra quelle individuate che contribuiscono a mitigare il rischio	62
4.4.5	Gravità del rischio, in relazione degli impatti potenziali e delle misure pianificate	64
4.4.6	Probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate	64
4.4.7	Valutazione complessiva	65
4.4.7.1	Valutazione	65
5	Convalida	65
5.1	Mappatura del rischio	66
5.2	Piano d'azione	66
5.2.1	Misure di rimedio e di miglioramento	67
	Integrare la protezione della privacy nei progetti	67
	Gestione del personale	67
		6

Controllo degli accessi	68
5.2.3 Nome del DPO e parere	68
5.2.4 Richiesta del parere degli interessati.	69
6. Documentazione	69

1 Gestione documento

Data	Autore	Versione	Descrizione
26.03.2026	Ing. Aristeo Marras	1.0	Predisposizione DPIA per il Trattamento dati personali per la segnalazione degli illeciti (Whistleblowing)
Data	Parere DPO	Versione	Descrizione
27.03.2026	Avv. Giovanni Battista Gallus	1.0	Parere del DPO sulla DPIA per il Trattamento dati personali per la segnalazione degli illeciti (Whistleblowing)
Data	Approvato da	Versione	Descrizione
30.03.2026	Ing. Riccardo Castrignanò	1.0	Approvazione del documento di DPIA per il Trattamento dati personali per la segnalazione degli illeciti (Whistleblowing)

2 Contesto

2.1 Ambito di applicazione

2.1.1 Trattamento oggetto della valutazione

Il Comune di Cagliari si caratterizza per una complessa realtà amministrativa che include servizi pubblici essenziali, gestione di personale esteso e rapporti con numerosi fornitori e collaboratori. Già dotato di un sistema whistleblowing, con la pubblicazione del Piano Triennale di Prevenzione della Corruzione e Trasparenza (PTPC) 2026-2028 l'Amministrazione ha avviato l'adeguamento degli strumenti alle normative più recenti per favorire l'emersione tempestiva di irregolarità e garantire integrità organizzativa.

In tale quadro, l'Amministrazione comunale ha realizzato un sistema strutturato di gestione delle segnalazioni (whistleblowing) interne volto a potenziare la trasparenza, supportare le attività del Responsabile Prevenzione Corruzione e Trasparenza (RPCT) e agevolare la verifica di condotte illecite. Il progetto è stato sviluppato nel rispetto del principio di "accountability" previsto dal Regolamento (UE) 2016/679 (GDPR), garantendo che il trattamento dei dati personali avvenga in modo lecito, proporzionato e trasparente.

L'iniziativa si inserisce in un percorso di adeguamento alla normativa nazionale sul whistleblowing (D.Lgs. 24/2023, attuazione Direttiva UE 2019/1937) e alle Linee Guida ANAC n. 478/2025, assicurando la tutela delle libertà individuali e il corretto equilibrio tra esigenze di integrità pubblica e protezione dei dati personali.

In tale contesto, essendo il Comune dotato di un Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) dedicato, la gestione del sistema di whistleblowing è affidato al medesimo, il quale, in adempimento alle prescrizioni e alle misure di sicurezza individuate dal Titolare e nell'ambito della normativa vigente, assicurano che il trattamento dei dati personali venga svolto nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche.

2.1.2 Obiettivi e metodologia applicata

Il presente documento rappresenta la Data Protection Impact Assessment effettuata dal Comune di Cagliari in ossequio all'art. 35 del Reg. UE 2016/679, in relazione al trattamento dei dati personali effettuato attraverso l'utilizzo del sistema strutturato di gestione delle segnalazioni whistleblowing interne, per la prevenzione della corruzione e trasparenza organizzativa.

La DPIA (Data Protection Impact Assessment) è una procedura obbligatoria prevista dall'art. 35 GDPR e art. 23 D.Lgs. 51/2018 per trattamenti che presentano rischi elevati per i diritti e le libertà delle persone fisiche. Ha l'obiettivo di descrivere il trattamento, valutarne necessità, proporzionalità e rischi per i diritti degli interessati, identificando misure idonee per mitigarli, applicabile a singoli o trattamenti analoghi.

Il GDPR (art. 24, 35, 36) e D.Lgs. 51/2018 (artt. 15, 23, 24) impongono al titolare di analizzare i rischi per adottare misure tecniche/organizzative adeguate, dimostrandone la conformità. Le Autorità di controllo, come il Garante italiano, possono elencare trattamenti che richiedono o escludono la DPIA. L'analisi precede l'avvio del trattamento, coinvolgendo il DPO; se, al termine dell'analisi, il rischio residuo sarà risultato elevato, si renderà necessaria la consultazione preventiva dell'Autorità.

Nel caso specifico, la DPIA è obbligatoria per i sistemi di whistleblowing, come espressamente chiarito dal Garante Privacy con riferimento ai trattamenti mediante applicativi per l'acquisizione e gestione delle segnalazioni illecite (art. 35 GDPR), data la particolare delicatezza delle informazioni trattate e gli elevati rischi ritorsivi/discriminatori per il segnalante.

Si fa presente che nell'esecuzione della DPIA è stato adottato un approccio metodologico in linea con quanto indicato dal CNIL e dagli standard riconosciuti a livello internazionale (es. Iso27001, ISO31000).

In particolare è stata adottata la seguente scala di valutazione in relazione alle misure adottate:

ACCETTABILE

Le misure adottate sono sufficienti a garantire la conformità normativa e la tutela dei dati personali degli interessati.

ACCETTABILE CON ELEMENTI DI MIGLIORAMENTO

Le misure adottate sono sufficienti a garantire la conformità normativa e la tutela dei dati personali degli interessati, pur in presenza di elementi consigliabili per aumentarne l'efficacia.

MIGLIORABILE

Le misure adottate sono parzialmente sufficienti a garantire la conformità normativa e la tutela dei dati personali degli interessati, per cui da integrare con ulteriori misure fortemente consigliate.

CRITICITA' CON AZIONI DI RIMEDIO

Le misure adottate non sono sufficienti a garantire la conformità normativa e la tutela dei dati personali degli interessati, con necessità di adottare misure specifiche.

E' obiettivo del Comune di Cagliari, aggiornare la presente DPIA sulla base di successive verifiche pianificate e di sostanziali cambiamenti di carattere normativo, tecnologico e organizzativo.

2.1.3 Responsabilità legate al trattamento

Titolare del trattamento

Il Titolare del trattamento è il Comune di Cagliari, in persona del Sindaco pro tempore, con sede in Via Roma 145 - 09124 Cagliari. Il Comune determina autonomamente le finalità e i mezzi del trattamento in questione, ai sensi dell'art. 4.7 del Reg. UE 2016/679.

Il Titolare è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali. A titolo esemplificativo e non esaustivo, si indicano i principali obblighi:

- 1) trattamento dei dati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- 2) divieto di trattamento dei dati ex art. 9 tranne nei casi di esenzione;
- 3) informare correttamente e in maniera trasparente gli interessati;
- 4) garantire il rispetto dei diritti degli interessati;
- 5) adottare le misure tecniche e organizzative adeguate a garantire, sin dalla fase della progettazione e per impostazione predefinita (privacy by design e by default), la tutela dei

diritti dell'interessato e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente;

- 6) vincolo al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;
- 7) fornire le istruzioni al responsabile del trattamento;
- 8) tenere il registro dei trattamenti;
- 9) fornire le istruzioni e formare il personale;
- 10) documentare la violazione dei dati personali, notificarle al Garante e comunicarle agli interessati nei casi previsti;
- 11) cooperare con l'autorità di controllo quando richiesto;
- 12) redigere le valutazioni di impatto nei casi previsti;
- 13) nominare il DPO.

Gestore delle segnalazioni (RPCT)

Il Comune nomina quale gestore delle segnalazioni per il sistema di whistleblowing il Responsabile Prevenzione Corruzione e Trasparenza (RPCT). Il Gestore delle segnalazioni sorveglia l'attuazione delle misure tecniche e organizzative di competenza, impartisce istruzioni operative, coordina la gestione della piattaforma e procede alla nomina delle persone autorizzate al trattamento.

Persone autorizzate

Le persone autorizzate al trattamento sono i collaboratori del RPCT espressamente nominati con atto formale. Tali soggetti possono accedere alle segnalazioni, dialogare con il segnalante (attraverso un codice univoco), effettuare attività di verifica, nel rispetto della procedura, delle istruzioni del titolare e delle procedure di tracciamento accessi.

Responsabili esterni e amministratori di sistema

Per la gestione tecnica della piattaforma (hosting cloud PNRR, GlobaLeaks, crittografia, manutenzione) il Comune nomina la società fornitrice Whistleblowing Solutions/Transparency International Italia come responsabile del trattamento ai sensi dell'art. 28 del GDPR.

Responsabile della Protezione dei Dati (DPO)

Il DPO è nominato ai sensi dell'art. 37 del GDPR. Fermo restando quanto previsto dall'art. 39 del GDPR in termini di responsabilità del DPO, ai fini del processo di esecuzione della DPIA, è compito del Responsabile per la protezione dei dati personali fornire un parere sulla medesima DPIA, qualora richiesto.

2.1.4 Normative e standard applicabili al trattamento

Regolamento UE 2016/679 (GDPR)

Il Regolamento UE 2016/679 (GDPR), applicabile dal 25 maggio 2018, rappresenta la normativa principale sulla protezione dei dati nell'UE, abrogando la precedente Direttiva 95/46/CE e imponendo a enti pubblici e privati – in qualità di Titolari o Responsabili del trattamento – l'obbligo di garantire la sicurezza delle operazioni sui dati personali. L'articolo 32 GDPR regola specificamente tale obbligo, richiedendo misure tecniche e organizzative adeguate al rischio (considerando stato dell'arte, costi, natura/contesto/finalità del trattamento e probabilità/gravità dei danni per diritti/libertà degli interessati). Tra queste: pseudonimizzazione/cifatura dei dati; garanzia permanente di riservatezza, integrità, disponibilità e resilienza dei sistemi; ripristino tempestivo dei dati in caso di incidenti; procedure regolari di test/verifica efficacia delle misure. La valutazione del rischio include minacce come distruzione, perdita, modifica, divulgazione non autorizzata o accessi accidentali/illegali. Il GDPR adotta un approccio risk-based, estendendo obblighi di sicurezza anche a Designati e Responsabili, e integrandoli con il principio di accountability: Titolari/Responsabili devono documentare conformità, istruire autorizzati (vietando trattamenti non istruiti, salvo norme UE/nazionali) e adottare misure stringenti proporzionali al rischio elevato. Codici di condotta (art. 40) o certificazioni (art. 41) facilitano la dimostrazione di compliance, enfatizzando riservatezza, integrità e disponibilità in ogni contesto operativo.

Ciò premesso, l'utilizzo del sistema strutturato di gestione delle segnalazioni di whistleblowing viene attuato nel rispetto dei principi applicabili al trattamento di dati personali di cui all'art. 5 del GDPR, nello specifico:

1. **Liceità:** il trattamento di dati personali effettuato attraverso il sistema di whistleblowing da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Esso, infatti, è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui i Comuni sono investiti, in particolare la prevenzione della corruzione e la promozione della trasparenza organizzativa.
2. **Proporzionalità:** nel commisurare la necessità del sistema di whistleblowing al grado di rischio concreto di illeciti, va evitato il trattamento di segnalazioni relative a doglianze personali o questioni non attinenti all'interesse pubblico. Il sistema può ricevere segnalazioni quando altre procedure interne (segnalazioni gerarchiche ordinarie) siano valutate insufficienti. La proporzionalità va valutata in ogni fase del trattamento, limitando i dati alle informazioni strettamente necessarie per la verifica.
3. **Finalità,** attuando il trattamento dei dati solo per scopi determinati ed espliciti. È consentito il whistleblowing come misura complementare volta a prevenire condotte illecite (penali,

amministrative, disciplinari) all'interno dell'ente, o che hanno lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del Titolare del trattamento o di terzi sulla base di segnalazioni fondate.

4. Necessità: la piattaforma è configurata per l'utilizzazione al minimo di dati personali e identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante segnalazioni anonime o opportune modalità che permettano di identificare il segnalante solo in caso di necessità.

Inoltre, ai sensi dell'Art. 32 del GDPR, per effettuare il trattamento devono essere adottate misure tecniche ed organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio. Le misure di sicurezza devono essere adeguate, è imposta quindi un'obbligazione di mezzi (non di risultato), in modo che siano ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi.

Gli standard internazionali relativi alla sicurezza delle informazioni indicano che la sicurezza dei dati non riguarda solo l'aspetto informatico del trattamento, ma anche l'aspetto organizzativo, a coprire eventi quali la sottrazione o la perdita dei dati e ogni altro evento che possa non renderli disponibili e/o alterarli. Le misure di sicurezza, quindi devono garantire il rispetto della riservatezza, integrità e disponibilità (RID), ovvero:

- i dati possano essere consultati, modificati, divulgati o cancellati solo dalle persone autorizzate
- i dati trattati siano accurati e completi in relazione alle finalità per cui sono trattati
- i dati rimangano accessibili e utilizzabili, cioè, in caso di perdita, modifica o distruzione accidentale, si deve essere in grado di recuperarli e prevenire danni alle persone interessate.

Legge n. 190 del 6 novembre 2012

La Legge 6 novembre 2012, n. 190 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", con la previsione dell'art. 1, comma 51, ha recepito le raccomandazioni di organismi internazionali inserendo l'art. 54-bis nel D.Lgs. 165/2001, garantendo la tutela del dipendente pubblico che segnala illeciti per favorire l'emersione di fattispecie illecite. Introduce il whistleblowing come strumento anticorruzione, basato sulla rivelazione non anonima di fatti corruttivi a autorità competenti, superando il dovere di fedeltà con buona fede e sospetti ragionevoli (Convenzione Consiglio Europa art.9)

Piano Nazionale Anticorruzione 2013 e ANAC Determina n.6/2015

Il Piano Nazionale Anticorruzione 2013 prevede che ogni amministrazione istituisca canali differenziati e riservati per segnalazioni, gestiti da ristretto personale con modelli sicuri per identificare autori illeciti.

L'ANAC con Determina n.6 del 28 aprile 2015 definisce la procedura whistleblowing, fornendo indicazioni operative e tutele per rimuovere ostacoli culturali (paura delazione/ritorsioni). L'aggiornamento PNA 2016 (Delibera 831/03.08.2016, punto 7.5) stimola segnalazioni e vieta discriminazioni da RPCT/vertici.

Legge n.179 del 30 Novembre 2017

La legge 30 novembre 2017, n. 179, recante “Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato”, pubblicata nella Gazzetta Ufficiale 14 dicembre 2017, n. 291, entrata in vigore dal 29 dicembre 2017, ha sostituito integralmente l'articolo 54-bis del decreto legislativo 30 marzo 2001, n. 165. La predetta disposizione normativa deve essere letta alla luce di due norme collaterali, e precisamente:

- l'articolo 331, comma 1, del codice di procedura penale che dispone: *“1. Salvo quanto stabilito dall'articolo 347, i pubblici ufficiali e gli incaricati di un pubblico servizio che, nell'esercizio o a causa delle loro funzioni o del loro servizio, hanno notizia di reato perseguibile di ufficio, devono farne denuncia per iscritto, anche quando non sia individuata la persona alla quale il reato è attribuito.”*
- l'articolo 8, del d.P.R. 16 aprile 2013, n. 62, rubricato *“Prevenzione della corruzione”* 1. *Il dipendente rispetta le misure necessarie alla prevenzione degli illeciti nell'amministrazione. In particolare, il dipendente rispetta le prescrizioni contenute nel piano per la prevenzione della corruzione, presta la sua collaborazione al responsabile della prevenzione della corruzione e, fermo restando l'obbligo di denuncia all'autorità giudiziaria, segnala al proprio superiore gerarchico eventuali situazioni di illecito nell'amministrazione di cui sia venuto a conoscenza.”.*

Decreto Legislativo n.24 del 10 Marzo 2023 e Linee guida ANAC

La tutela dei segnalanti è stata ulteriormente rafforzata, dal Decreto Legislativo n. 24 del 10/03/2023, con la possibilità di effettuare segnalazioni esterne all'ANAC o alle autorità competenti, nonché la divulgazione pubblica in casi specifici. Inoltre, il suddetto decreto ha rafforzato le misure di protezione contro le ritorsioni, il divieto di atti discriminatori e ha introdotto l'inversione dell'onere della prova in caso di presunta ritorsione. Infatti l'art. 17 c.2 prevede “Nell'ambito di procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati ai sensi del presente articolo nei confronti delle persone di cui all'articolo 3, commi 1, 2, 3 e 4, si presume che gli stessi siano stati posti in essere a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione, alla divulgazione pubblica o alla denuncia è a carico di colui che li ha posti in essere.”.

Inoltre, la protezione è stata estesa anche a collaboratori, fornitori, che possano essere venuti a conoscenza di illeciti durante il rapporto lavorativo.

Il decreto, inoltre, ha previsto un ruolo centrale per l'ANAC, che ha il compito di attivare il canale di segnalazione esterna, tramite piattaforma informatica. Tale obbligo si è concretizzato con l'approvazione delle Linee Guida ANAC con Delibera n. 311 del 12/07/2023, modificata ed integrata dalla delibera n. 479 del 26 novembre 2025 "Modifica ed integrazione della Delibera n. 311 del 12 luglio 2023 recante "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

Provvedimenti Garante Privacy

Il Garante per la Protezione dei Dati Personali ha stabilito l'obbligatorietà della DPIA per tutti i sistemi di whistleblowing con l'Ordinanza ingiunzione n. 9768363 del 7 aprile 2022 [9768363], riconoscendo che tali trattamenti presentano rischi specifici ed elevati per i diritti e le libertà degli interessati ex art. 35.3 GDPR. L'Autorità ha chiarito che le piattaforme di gestione segnalazioni comportano rischio intrinseco alto per il trattamento sistematico di categorie particolari di dati (artt.9-10 GDPR: salute, reati penali, opinioni) unitamente alla vulnerabilità del segnalante, esposto a ritorsioni lavorative in contesto gerarchico.

Tale principio è ribadito nel successivo Parere n. 581 del 9 ottobre 2025 [10184673] sugli schemi Linee Guida ANAC 478/2025.

2.1.4.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Gli standard e le normative riferibili al trattamento sono correttamente individuati e monitorati. Il trattamento effettuato tramite il sistema di gestione delle segnalazioni (Whistleblowing) oggetto della presente DPIA è valutato in conformità al quadro normativo applicabile.

2.2 Dati, processi e risorse di supporto

2.2.1 Tipologie di dati trattati

Il sistema di gestione delle segnalazioni di whistleblowing del Comune di Cagliari tratta principalmente dati personali contenuti nelle segnalazioni interne, raccolti tramite piattaforma WhistleblowingIT basata su GlobaLeaks (<https://comunecagliari.whistleblowing.it/>) e canali orali (verbalizzazioni RPCT), inclusi metadati tecnici e allegati documentali.

Categorie principali di dati:

- a) Dati identificativi segnalante (opzionali, ma raccomandati per dialogo bidirezionale): nome, cognome, qualifica/funzione, email/telefono ruolo, codice univoco 16 cifre (non nominativo)
- b) Dati identificativi segnalato/terzi: nome, cognome, qualifica, servizio di appartenenza, elementi identificativi (per verifiche)
- c) Dati sul contenuto segnalazione: descrizione fatti illeciti (penali: corruzione, peculato; amministrativi/disciplinari), tempo/luogo, testimoni, allegati documentali (PDF, immagini)
- d) Dati sensibili/particolari: reati penali (art.10 GDPR), salute/sicurezza lavoratori (art.9), opinioni politiche/sindacali, origine etnica/religiosa (incidentalmente rilevabili da contesto)
- e) Metadati tecnici: timestamp invio, IP anonimo (non tracciabile), tipo dispositivo, log accessi RPCT (accesso/contenuti, non identificativi)
- f) Dati pseudonimizzati: codice univoco per dialogo segnalante-RPCT (bidirezionale sicuro).

2.2.2 Ciclo di vita del trattamento dei dati

Il ciclo di vita del trattamento dei dati nel sistema di whistleblowing del Comune di Cagliari inizia con la raccolta delle segnalazioni che può avvenire tramite due canali distinti:

- Canale scritto tramite la piattaforma WhistleblowingIT, basata su GlobaLeaks (<https://comunecagliari.whistleblowing.it/>): il segnalante procede alla compilazione di un questionario guidato per effettuare in autonomia la segnalazione.
- Canale orale, tramite richiesta inviata alla mail del RPCT per un incontro con il RPCT entro 30 giorni, con verbalizzazione e successivo inserimento della segnalazione nella piattaforma WhistleblowingIT basata su GlobaLeaks da parte del gestore.

Dopo la fase di raccolta sulla piattaforma, i dati vengono sottoposti dal gestore (RPCT) a valutazione preliminare per verificarne ammissibilità e procedibilità, seguita dall'istruttoria con accertamenti, verifiche e possibili integrazioni da parte del segnalante.

Durante l'istruttoria, il RPCT può condividere informazioni anonimizzate e minimizzate con altre funzioni interne o esperti esterni (es. specialisti informatici, giuristi), limitatamente alle attività di competenza

I dati vengono trasmessi in forma crittografata e memorizzati per un periodo di 12 mesi (estendibile fino a un massimo di 5 anni dalla comunicazione dell'esito delle attività di accertamento al segnalante), con cancellazione automatica alla scadenza.

Come previsto nel PTPC 2026-2028, i termini di conservazione sono stabiliti sulla base dei principi di necessità, pertinenza e non eccedenza (art.5.1 e GDPR), in ragione delle diverse tipologie di dati trattati (identificativi, sensibili art.9-10) e delle finalità perseguite, in conformità a D.Lgs.24/2023 e Linee Guida ANAC 478/2025.

Il sistema GlobaLeaks è programmato per operare, al momento prefissato, l'integrale cancellazione automatica delle segnalazioni da ogni supporto, con modalità che rendono i dati non riutilizzabili (cifatura + eliminazione irreversibile), garantendo privacy by design.

2.2.3 Risorse di supporto ai dati

Il sistema di whistleblowing del Comune di Cagliari utilizza la piattaforma WhistleblowingIT di Transparency International Italia e Whistleblowing Solutions, basata su GlobaLeaks open-source in versione cloud PNRR qualificato (<https://comunecagliari.whistleblowing.it/>), migrata dalla precedente infrastruttura interna per conformità al D.Lgs. 24/2023 e Linee Guida ANAC n. 478/2025.

Componenti infrastrutturali principali:

- Piattaforma GlobaLeaks con questionario guidato (domande aperte/chiose obbligatorie), upload allegati sicuri e dialogo bidirezionale tramite codice univoco a 16 cifre.
- Crittografia end-to-end per protezione dati in transito e at-rest, inaccessibili a non autorizzati.
- Hosting cloud certificato ACN (AgID Cloud Nazionale), senza server fisici interni.
- Accessi autorizzati limitati a RPCT e collaboratrice, con autenticazione 2FA.

Canali di acquisizione:

- Scritto (H24): piattaforma web accessibile da qualsiasi rete, non tracciabile.
- Orale: richiesta incontro RPCT, fissato entro 30 giorni, con verbalizzazione da parte del gestore sulla piattaforma (registrazione solo su consenso). I dati confluiscono automaticamente nella piattaforma cloud (RPD: Whistleblowing Solutions/Transparency International), accessibile esclusivamente da RPCT/staff autorizzato; la Centrale Operativa (ufficio RPCT) gestisce ricezione, dialogo bidirezionale, coordinamento verifiche (interne/esterne con dati anonimizzati) e riscontro al segnalante entro 3 mesi.

2.2.3.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
I trattamenti in esame e il ciclo di vita dei dati sono stati individuati correttamente in modo conforme alla normativa di riferimento. Ogni cambiamento è monitorato e periodicamente recepito nei documenti di riferimento.

3 Principi Fondamentali

3.1 Finalità, proporzionalità, necessità

3.1.1 Finalità del trattamento

La raccolta, la registrazione, la conservazione e, in generale, il trattamento dei dati personali contenuti nelle segnalazioni di whistleblowing avvengono esclusivamente per le seguenti finalità:

- Prevenzione e contrasto della corruzione ai sensi della L.190/2012 e D.Lgs.24/2023.
- Tutela della trasparenza e integrità organizzativa del Comune di Cagliari.
- Verifica fondatezza segnalazioni illecite (penali, amministrativi, disciplinari).
- Esecuzione obblighi PTPC 2026-2028.
- Attivazione procedimenti disciplinari/amministrativi se fondate.
- Denuncia autorità giudiziarie/contabili per illeciti penali/danno erariale.
- Adempimento obblighi ANAC (Linee Guida 478/2025).

Le finalità del trattamento sono specifiche in quanto il titolare non effettua alcun trattamento sui dati personali raccolti per il perseguimento di finalità differenti da quelle indicate nel presente documento e nell'informativa e procedura whistleblowing.

Gli scopi del trattamento sono espliciti e legittimi in quanto vengono preventivamente resi noti ai soggetti interessati tramite:

- Informativa art.13 GDPR pubblicata sulla piattaforma <https://comunecagliari.whistleblowing.it/>
- Procedura PTPC 2026-2028 (pubblicamente disponibile).
- Questionario guidato GlobalLeaks con spiegazione finalità/ambito applicazione.

All'interno dell'informativa vengono esplicitati gli scopi del trattamento e tutte le indicazioni previste dall'articolo 13 del Regolamento UE 679/2016, inclusa l'indicazione delle modalità di trattamento (piattaforma scritta/orale), base legale (art.6.1.c obbligo D. Lgs.24/2023), periodo conservazione (max 5 anni), diritti esercitabili e contatti RPCT/DP.

3.1.2 Basi giuridiche del trattamento

La base giuridica del trattamento è rappresentata dall'art. 6, comma 1, lett. c), del Regolamento UE 2016/679 (*"il trattamento è necessario per l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento"*).

Inoltre, i dati personali sono trattati dal Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) nell'esecuzione dei propri compiti obbligatori, con particolare riferimento all'obbligo di attivare e gestire canali interni di segnalazione ai sensi dell'art. 4 D.Lgs. 24/2023 (attuazione Direttiva UE 2019/1937), che recepisce e amplia l'art. 54-bis del D.Lgs. n. 165/2001 (modificato L.179/2017).

Tale base giuridica è concretizzata dal PTPC Cagliari 2026-2028 (Allegato 2.3.A4), che designa il Responsabile della prevenzione della corruzione e trasparenza come gestore, responsabile della ricezione, verifica e gestione delle segnalazioni.

L'obbligo legale cogente esclude discrezionalità del titolare e legittima il trattamento di dati sensibili (artt.9-10 GDPR) per finalità di prevenzione corruzione, trasparenza e accertamento illeciti penali/amministrativi/disciplinari di interesse pubblico.

3.1.3 Minimizzazione dei dati trattati

I dati personali raccolti sono adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati, nel rispetto del principio di "minimizzazione dei dati" dettato dall'art. 5, par. 1, lett. c), del Reg. UE 2016/679.

Il sistema di whistleblowing del Comune di Cagliari adotta il principio di minimizzazione raccogliendo solo le informazioni strettamente necessarie per verificare segnalazioni illecite di interesse pubblico, tramite questionario guidato GlobaLeaks che esclude doglianze personali, relazioni interpersonali o questioni non attinenti a corruzione/illeciti penali/amministrativi/disciplinari. L'informativa art.13 sulla piattaforma specifica l'ambito applicativo, informando gli interessati dell'attività di trattamento.

L'attività di gestione segnalazioni raccoglie solo i dati indispensabili:

- Segnalante: codice univoco 16 cifre (pseudonimo), dati personali opzionali per dialogo (nome/ email/ ruolo/ numero di telefono).
- Contenuto: descrizione fattispecie, tempo/luogo, testimoni essenziali, allegati probatori pertinenti e limitati.
- Segnalato: identificativi minimi (nome/qualifica/servizio) per successive verifiche.

La piattaforma è impostata per minimizzare il trattamento di dati personali e include: questionario a tendina predefinita, allegati compressi/cifrati, no campi liberi non necessari, nel rispetto dei principi di pertinenza e non eccedenza. Il Rilevamenti di ulteriori dati sensibili (artt.9-10 GDPR) possono avvenire solo in via accidentale e occasionale per contesto segnalazione, con anonimizzazione verifiche interne.

3.1.4 L'accuratezza e l'attualità dei dati

Il meccanismo di gestione e sovrascrittura automatica dei dati garantisce il loro costante aggiornamento e la limitazione della quantità dei dati trattati, in conformità al principio di accuratezza (art. 5, par. 1, lett. d), GDPR).

La piattaforma WhistleblowingIT basata su GlobaLeaks adotta cancellazione automatica programmata alla scadenza dei termini (12 mesi di default, estendibile fino a un max di 5 anni dalla data di comunicazione dell'esito finale), con eliminazione irreversibile mediante sovrascrittura crittografica, impedendo recuperi accidentali o non autorizzati.

L'accuratezza dei dati è assicurata dalla verifica del RPCT: le segnalazioni vengono validate per fondatezza (analisi dei documenti allegati, riscontri oggettivi), con archiviazione immediata delle infondate e aggiornamento procedurale delle fondate (esiti disciplinari/giudiziari comunicati al segnalante tramite codice univoco). Eventuali rettifiche sono annotate nel fascicolo digitale con timestamp immutabile, mantenendo integralità e tracciabilità del processo.

Tale meccanismo garantisce che i dati trattati riflettano lo stato attuale delle verifiche e siano cancellati tempestivamente una volta esaurite le finalità, nel rispetto del principio di limitazione della conservazione (art. 5, par. 1, lett. e), GDPR).

3.1.5 Durata della conservazione dei dati

Come previsto nel PTPC 2026-2028, i termini di conservazione sono stabiliti sulla base dei principi di necessità, pertinenza e non eccedenza (art.5.1. e GDPR), in ragione delle diverse tipologie di dati personali trattati (identificativi, sensibili artt.9-10) e tenendo conto di ciascuna finalità perseguita (ricezione, verifica, feedback), in conformità a D. Lgs.24/2023 e alle Linee Guida ANAC n.478/2025.

In particolare, i dati delle segnalazioni whistleblowing richiedono conservazione per un periodo congruo al completamento delle verifiche e del riscontro al segnalante, tenendo conto delle tempistiche investigative e degli obblighi di conservazione probatoria per accertamento illeciti penali/amministrativi.

Il sistema GlobaLeaks è programmato per operare, al momento prefissato, l'integrale cancellazione automatica delle informazioni da ogni supporto, anche mediante sovrascrittura crittografica, con modalità tali da rendere non riutilizzabili i dati cancellati (retention default 12 mesi estendibile fino a un max di 5 anni dalla comunicazione dell'esito finale).

Tale impostazione garantisce proporzionalità alla natura delle segnalazioni e conformità agli obblighi normativi, con cancellazione tempestiva una volta esaurite le finalità del trattamento.

3.1.6 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Il trattamento è effettuato nel rispetto dei principi fondamentali. In particolare, i trattamenti perseguono scopi legittimi e le basi giuridiche sono individuate in modo conforme alla normativa vigente. I tempi di conservazione dei dati sono individuati e risultano conformi alla normativa applicabile.

3.2 Controlli per proteggere i diritti personali dei soggetti interessati

3.2.1 Le modalità di informativa ai soggetti interessati

Ai sensi dell'art. 13 del Reg. UE 2016/679, il titolare del trattamento fornisce agli interessati dettagliate informazioni in merito al trattamento dei dati, l'informazione agli interessati è assicurata attraverso differenti strumenti:

- 1) Informativa pubblicata nella sezione trasparenza del sito istituzionale del Comune di Cagliari.
- 2) Informativa pubblicata direttamente sulla piattaforma WhistleblowingIT, basata su GlobaLeaks <https://comunecagliari.whistleblowing.it/>, visibile immediatamente al potenziale segnalante prima dell'invio questionario.
- 3) PTPC 2026-2028 pubblicato sul sito istituzionale del Comune di Cagliari, con dettagli operativi e modello segnalazione.
- 4) Canale orale: informativa verbale preliminare durante appuntamento RPCT, con consegna copia informativa scritta.

L'informativa completa contiene tutti i dati previsti dall'art. 13 del Reg. UE 2016/679 ed è a disposizione degli interessati con modalità di facile accesso.

3.2.2 Raccolta del consenso dei soggetti interessati

Il trattamento dei dati non è basato sul consenso degli interessati essendo i trattamenti necessari per l'adempimento a un obbligo legale (art. 6, paragrafo 1, lettera c del GDPR 679/16 e art. 4 del D.Lgs. 24/2023).

Gli interessati sono liberi di non inviare segnalazioni, ma l'ente è obbligato a garantire i canali per chi voglia farlo volontariamente.

3.2.3 Modalità di esercizio del diritto di accesso ai dati da parte dei soggetti interessati

I soggetti interessati (segnalanti, segnalati, testimoni) possono esercitare i loro diritti di accesso (art.15 GDPR) attraverso le modalità indicate nell'informativa art.13 GDPR pubblicata sulla piattaforma <https://comunecagliari.whistleblowing.it/> e nel PTPC.

Modalità di esercizio:

- Invio richiesta scritta a RPCT via mail
- Identificazione con copia documento identità (art.12.6 GDPR).

Gestione richieste:

- Risposta entro 1 mese dal ricevimento (art.12.3 GDPR), prorogabile a 3 mesi per complessità
- La richiesta sarà gestita in accordo con il DPO, ove necessario.

Limitazioni legali (art.23 GDPR + D.Lgs.24/2023):

- Tutela segnalante: divieto rivelazione identità (art.4 D.Lgs.24/2023), pseudonimizzazione dati estratti.

- Segnalato: accesso limitato a dati personali strettamente riferibili, con anonimizzazione segnalante.
- Terzi: esclusione da risposte se non direttamente coinvolti.
- Indagini in corso: differimento accesso per tutela investigativa (art.2-quinquies D. Lgs.196/2003).
- Casi di impossibilità identificazione: Segnalazioni anonime: non identificabili.

Il personale RPCT garantisce gestione conforme tempi e modalità GDPR, con tracciamento irrevocabile delle risposte nel registro art.30.

3.2.4 Modalità di esercizio del diritto alla rettifica e alla cancellazione dei dati da parte dei soggetti interessati

I soggetti interessati (segnalanti, segnalati, testimoni) esercitano i diritti alla rettifica (art.16 GDPR) e cancellazione ("oblio", art.17 GDPR) secondo le indicazioni dell'informativa art.13 pubblicata su <https://comunecagliari.whistleblowing.it/> e nel PTPC 2026-2028.

Modalità di esercizio:

- Invio richiesta scritta a RPCT via mail
- Identificazione con copia documento identità (art.12.6 GDPR).

Gestione richieste:

- Risposta entro 1 mese dal ricevimento (art.12.3 GDPR), prorogabile a 3 mesi per complessità.
- La richiesta sarà gestita in accordo con il DPO, ove necessario.

Limitazioni legali (art.23 GDPR e D. Lgs.24/2023):

- Tutela investigativa: divieto cancellazione durante procedimenti GdF/Procura.
- Obblighi probatori: conservazione atti disciplinari/giudiziari pendenti.

3.2.5 Modalità di esercizio del diritto di limitazione e opposizione dei dati da parte dei soggetti interessati

I soggetti interessati (segnalanti, segnalati, testimoni) esercitano i diritti di limitazione del trattamento (art.18 GDPR) e opposizione (art.21 GDPR) secondo le indicazioni dell'informativa art.13 su <https://comunecagliari.whistleblowing.it/> e PTPC 2026-2028.

Modalità di esercizio:

- Invio richiesta scritta a RPCT via mail
- Identificazione con copia documento identità (art.12.6 GDPR).

Gestione richieste:

- Risposta entro 1 mese dal ricevimento (art.12.3 GDPR), prorogabile a 3 mesi per complessità.
- La richiesta sarà gestita in accordo con il DPO, ove necessario.

Limitazioni legali (art.23 GDPR e D. Lgs.24/2023):

Limitato fortemente da interessi pubblici prevalenti:

- Prevenzione corruzione (L.190/2012).
- Verifica illeciti interesse pubblico (D. Lgs.24/2023).
- Obblighi PTPC + ANAC 478/2025.

Ai sensi dell'art. 2-undecies D.Lgs. 196/2003, i diritti di cui agli artt. 15-22 GDPR non possono essere esercitati qualora dall'esercizio possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte. L'esercizio di tali diritti potrà essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato. In tale caso, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità previste dall'art. 160 D.Lgs. 196/2003.

3.2.6 Obblighi dei responsabili del trattamento

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da contratti formali conformi all'art. 28 Reg. UE 2016/679, sottoscritti dal Comune di Cagliari con Whistleblowing Solutions S.r.l./Transparency International Italia (gestore piattaforma GlobalLeaks su cloud PNRR).

WhistleblowingIT, nominato come responsabile esterno, ha accesso esclusivamente a metadati tecnici per manutenzione piattaforma, con divieto assoluto accesso contenuti segnalazioni. L'accesso dei contenuti è riservato solo al Responsabile della prevenzione della corruzione e trasparenza e staff, autenticati tramite 2FA.

Il contratto disciplina:

- Istruzioni scritte del titolare: gestione tecnica, no elaborazione contenuti.
- Misure sicurezza: crittografia end-to-end, audit annuali ACN cloud.
- Sottotrattanti autorizzati: solo Transparency International.
- Durata: 12 mesi rinnovabile, eliminazione irreversibile dati a cessazione.
- Audit RPCT: diritto verifica conformità su richiesta.

Le nomine hanno valore contrattuale, sono sottoscritte, archiviate e disponibili per interessati (art.15 GDPR), garantendo accountability e conformità Linee Guida ANAC 478/2025.

3.2.7 Protezione dei dati nel caso di trasferimento di dati fuori dall'Unione Europea

I dati personali raccolti non sono trasferiti al di fuori dell'Unione Europea o di stati ritenuti "trust" da parte della Commissione Europea.

Nel caso in cui, per esigenze organizzative, fosse necessario il trasferimento anche al di fuori dell'Unione Europea, il Titolare assicura che avverrebbe in conformità alle disposizioni di legge applicabili, previa stipula delle clausole contrattuali standard previste dalla Commissione Europea.

3.2.8 Valutazione

VALUTAZIONE
ACCETTABILE CON ELEMENTI DI MIGLIORAMENTO
COMMENTO DI VALUTAZIONE
I soggetti interessati sono informati adeguatamente e possono esercitare i loro diritti in modo conforme alla normativa. Si suggerisce la definizione e adozione di una procedura per la gestione dei diritti degli interessati.

4 Rischi

4.1 Controlli esistenti o pianificati

4.1.1 Crittografia

La piattaforma WhistleblowingIT basata su GlobaLeaks del Comune di Cagliari opera su infrastruttura cloud PNRR qualificata ACN livello 1 (<https://comunecagliari.whistleblowing.it/>), con crittografia end-to-end nativa per tutti i flussi dati in ingresso/uscita e a riposo.

La trasmissione avviene tramite protocollo HTTPS/TLS sicuro, garantendo confidenzialità e integrità. I dati memorizzati sul cloud utilizzano cifratura AES-256 at-rest gestita dal provider WhistleblowingIT, accessibile solo tramite autenticazione 2FA da parte del RPCT.

L'allegato crittografico dei documenti probatori (PDF, immagini) è automatico al caricamento, con chiavi gestite esclusivamente dal cloud provider. Il contratto art.28 GDPR con Whistleblowing Solutions disciplina standard minimi sicurezza, garantendo separazione logica da altri servizi cloud e conformità privacy by design ex art.32 GDPR.

Canale orale (incontro RPCT): nessuna registrazione salvo consenso specifico, verbalizzazione manuale all'interno dell'applicativo software eseguita dal RPCT crittografata digitalmente.

4.1.1.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.2 Anonimizzazione

Le segnalazioni whistleblowing possono essere effettuate in forma anonima, senza obbligo di fornire dati identificativi del segnalante, garantendo così la massima riservatezza.

Tuttavia, per accedere alle tutele specifiche previste dal D.Lgs. 24/2023 (protezione da ritorsioni) e facilitare il dialogo bidirezionale con il RPCT tramite codice univoco a 16 cifre, nonché per supportare accertamenti e procedimenti, si raccomanda vivamente di condividere volontariamente dati personali limitati (nome, qualifica, servizio).

Il Riconoscimento delle persone avviene solo tramite dati forniti volontariamente nella segnalazione (nome, qualifica, servizio), limitati allo stretto necessario per accertamenti RPCT.

Pseudonimizzazione implementata:

- Segnalante: codice univoco 16 cifre (non invertibile).
- Verifiche interne: oscuramento identificativi non essenziali.
- Comunicazioni autorità: anonimizzazione completa del segnalante (art.4 D. Lgs.24/2023).

Tale impostazione garantisce equilibrio tra necessità investigative e tutela privacy, con pseudonimizzazione come misura di sicurezza proporzionata (art.32 GDPR) in luogo dell'anonimizzazione irreversibile.

4.1.2.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.3 Partizionamento dei dati

La piattaforma WhistleblowingIT basata su GlobalLeaks opera come sistema monolitico all'interno di ciascuna istanza dedicata per ente (architettura cloud multi-tenant con partizionamento logico/database separati tra clienti diversi per garantire isolamento GDPR-compliant). Non sono previsti partizionamenti specifici per tipologia di dati trattati nelle segnalazioni whistleblowing (testo, allegati documentali, metadati tecnici). L'accesso granulare è gestito tramite ruoli RBAC (Role-Based Access Control).

4.1.3.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE

Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.4 Controllo degli accessi logici

Nel sistema di whistleblowing del Comune di Cagliari, il controllo degli accessi logici è regolato tramite credenziali dedicate univoche sulla piattaforma WhistleblowingIT basata su GlobalLeaks cloud PNRR (<https://comunecagliari.whistleblowing.it/>), con autenticazione a due fattori (2FA) obbligatoria per tutti gli utenti autorizzati.

Utenti autorizzati e profili:

- Responsabile per la prevenzione della corruzione e trasparenza: profilo "ricevente gestione completa" (visualizzazione, dialogo bidirezionale, assegnazione verifiche).
- Staff RPCT: stesso profilo, accesso limitato segnalazioni condivise dal gestore.

Sistema autenticazione:

- Username/password univoci + 2FA (SMS/app autenticatore).
- No accessi condivisi: credenziali personali non trasferibili.
- Revoca automatica: disattivazione immediata cessazione rapporto.

4.1.4.1 Valutazione

VALUTAZIONE
ACCETTABILE CON ELEMENTI DI MIGLIORAMENTO
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato. Si consiglia una definizione e attuazione di una password policy strutturata e di monitorarne la corretta applicazione.

4.1.5 Tracciabilità

Nella piattaforma WhistleblowingIT basata su GlobaLeaks del Comune di Cagliari, la tracciabilità è garantita dalla registrazione automatica di tutte le operazioni effettuate sulla piattaforma cloud PNRR, che documenta accessi, visualizzazioni segnalazioni, dialoghi bidirezionali, esportazioni allegati e assegnazioni verifiche associate alle credenziali uniche degli utenti autorizzati.

I log di sistema della piattaforma registrano automaticamente tutte le attività del profilo "ricevente", identificando precisamente:

- Accessi piattaforma: timestamp e conferma 2FA.
- Visualizzazioni: segnalazioni aperte (testo e allegati).
- Dialoghi: messaggi bidirezionali (codice univoco 16 cifre).
- Esportazioni: download documenti probatori.
- Assegnazioni: trasferimenti verifiche interne.

I log tecnici sono conservati 12 mesi con cancellazione automatica irreversibile, accessibili esclusivamente al RPCT tramite 2FA, supportando audit interni e indagini su data breach.

4.1.5.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.6 Archiviazione

Nel sistema di whistleblowing del Comune di Cagliari, l'archiviazione dei dati avviene sulla piattaforma WhistleblowingIT basata su GlobaLeaks cloud PNRR qualificata ACN Livello 1 (SA-172) (<https://comunecagliari.whistleblowing.it/>), gestita da Whistleblowing Solutions S.r.l., senza hardware dedicato locale. La piattaforma cloud offre capacità illimitata con archiviazione automatica crittografata, dove vengono registrate segnalazioni, allegati documentali e log tecnici con cancellazione automatica programmata dopo 12 mesi (estendibile fino a un max di 5 anni dall'esito della segnalazione). Questa configurazione su infrastruttura AgID Cloud Nazionale assicura integrità, disponibilità e resilienza dei dati durante l'intero ciclo di vita, con segregazione logica

automatica per tenant (Comune Cagliari separato da altri enti), eliminando rischi di esposizione fisica o interferenze rete comunale.

4.1.6.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
I tempi di conservazione dei dati sono stati determinati sulla base delle finalità perseguite.

4.1.7 Sicurezza dei documenti cartacei

Il sistema di whistleblowing del Comune di Cagliari opera esclusivamente in formato digitale tramite la piattaforma WhistleblowingIT basata su GlobaLeaks cloud PNRR (<https://comunecagliari.whistleblowing.it/>), senza prevedere trascrizioni cartacee dei dati trattati. Anche per il canale orale, le verbalizzazioni dell'incontro con il segnalante vengono redatte digitalmente dal RPCT con firma elettronica qualificata e caricate direttamente sulla piattaforma GlobaLeaks nella sezione dedicata alla segnalazione specifica, dove rimangono archiviate nel cloud cifrato senza alcuna stampa cartacea.

Non sono previste trascrizioni cartacee dei dati oggetto di questo trattamento.

4.1.7.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura accettabile sulla base delle finalità perseguite e modalità di trattamento.

4.1.8 Minimizzazione dei dati

La raccolta dei dati nella piattaforma WhistleblowingIT basata su GlobaLeaks del Comune di Cagliari è strettamente limitata ai dati indispensabili per le finalità del trattamento previsto dall'art. 5 par. 1 lett. c) GDPR, limitandosi alle informazioni essenziali per l'identificazione e la gestione delle segnalazioni whistleblowing (D.Lgs. 24/2023), in linea con quanto definito nella procedura di gestione delle segnalazioni.

La piattaforma raccoglie esclusivamente allegati forniti volontariamente dal segnalante, senza alcuna acquisizione automatica di flussi video o immagini. I campi anonimi obbligatori richiedono solo descrizione dei fatti, contesto e prove documentali, evitando qualsiasi dato identificativo non strettamente pertinente alla segnalazione.

Questa impostazione privacy by design (art.25 GDPR) riduce al minimo l'esposizione dei dati personali, limitando gli scambi nel dialogo protetto alle informazioni essenziali e consentendo download selettivi solo dei documenti probatori necessari, garantendo così proporzionalità e non eccedenza (art.5.1.c GDPR).

4.1.8.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.9 Vulnerabilità

La piattaforma WhistleblowingIT basata su GlobaLeaks cloud PNRR del Comune di Cagliari è stata oggetto di analisi per identificare potenziali vulnerabilità tecniche e organizzative che potrebbero compromettere la sicurezza dei dati personali trattati.

La qualificazione ACN livello 1 (SA-172) supportata dalle certificazioni ISO 27001:2022, 27017 e 27018, esprime una gestione strutturata del processo di vulnerability management.

Le componenti software mantengono aggiornamenti firmware automatici dal provider Whistleblowing Solutions S.r.l.

Tale configurazione garantisce resilienza completa e conformità art.32 GDPR, Direttiva NIS2, Linee Guida ANAC 478/2025.

4.1.9.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misure di sicurezza accettabile in relazione al trattamento effettuato.

4.1.9 Lotta contro il malware

La piattaforma WhistleblowingIT basata su GlobalLeaks cloud PNRR qualificata ACN SA-1721 Livello 1 del Comune di Cagliari implementa protezioni multilivello contro malware come parte integrante della qualificazione ACN, supportata dalle certificazioni ISO 27001:2022, 27017 e 27018.

Gli allegati (documenti probatori, immagini) sono sottoposti a controlli automatici e validazione prima dell'archiviazione crittografata, con isolamento dei file sospetti per prevenire propagazione o esecuzione malevola.

L'infrastruttura del provider Whistleblowing Solutions S.r.l., certificata ISO 27001, garantisce sicurezza perimetrale e resilienza contro minacce informatiche, in conformità con art.32 GDPR e Direttiva NIS2.

4.1.10.1 Valutazione

VALUTAZIONE

ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al Trattamento effettuato.

4.1.11 Gestione postazioni

Nel sistema di whistleblowing del Comune di Cagliari, la gestione delle postazioni avviene con accesso esclusivamente in remoto tramite piattaforma WhistleblowingIT basata su GlobalLeaks cloud PNRR (<https://comunecagliari.whistleblowing.it/>), senza postazioni fisiche dedicate.

Nessuna postazione fisica dedicata né interfacce locali. L'architettura cloud elimina hardware specifico, garantendo accesso controllato con tracciamento completo (timestamp, IP, azioni) conforme art.32 GDPR

4.1.11.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.12 Sicurezza dei siti web

La piattaforma WhistleblowingIT basata su GlobalLeaks cloud PNRR qualificata ACN SA-1721 Livello 1 (<https://comunecagliari.whistleblowing.it/>) del Comune di Cagliari implementa sicurezza web certificata tramite certificazioni ISO 27001:2022, 27017 e 27018.

Il servizio è esposto su Private Cloud Seeweb Milano Caldera con connettività ridondata e standard OWASP, W3C, IETF, garantendo protezione contro accessi non autorizzati e attacchi web comuni.

4.1.12.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.13 Backup

La piattaforma WhistleblowingIT basata su GlobalLeaks cloud PNRR qualificata ACN SA-1721 Livello 1 del Comune di Cagliari implementa procedure di backup automatiche gestite dal provider Whistleblowing Solutions S.r.l.

La piattaforma cloud esposta su Private Cloud Seeweb Milano Caldera garantisce ridondanza dati durante tutto il periodo di retention per segnalazioni, allegati documentali e log tecnici, supportata dalle certificazioni ISO 27001:2022, 27017 e 27018.

Le esportazioni sicure dei documenti probatori sono disponibili esclusivamente per RPCT tramite interfaccia web protetta 2FA, con tracciamento completo di tutte le operazioni.

Tale gestione cloud centralizzata assicura disponibilità e resilienza dei dati conforme art.32 GDPR.

4.1.13.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.14 Manutenzione

La manutenzione della piattaforma WhistleblowingIT basata su GlobaLeaks cloud PNRR qualificata ACN SA-1721 Livello 1 del Comune di Cagliari è gestita autonomamente dal provider Whistleblowing Solutions S.r.l., con aggiornamenti software costanti per adeguamento normativo.

4.1.14.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza parzialmente accettabile in relazione al trattamento effettuato.

4.1.15 Contratto con il responsabile del trattamento

Whistleblowing Solutions S.r.l. è nominata Responsabile del trattamento ex art. 28 GDPR per la gestione della piattaforma basata su GlobaLeaks cloud PNRR qualificata ACN SA-1721 Livello 1 del Comune di Cagliari.

Gli obblighi del Responsabile sono definiti nel contratto di servizio che recepisce art. 28 GDPR, includendo garanzie basate su certificazioni ISO 27001:2022, 27017, 27018, standard OWASP e connettività ridondata Private Cloud Seeweb Milano Caldera. La nomina è archiviata nella documentazione privacy comunale.

WhistleblowingIT, nominato come responsabile esterno, ha accesso esclusivamente a metadati tecnici per manutenzione piattaforma, con divieto assoluto accesso contenuti segnalazioni. L'accesso dei contenuti è riservato solo al Responsabile della prevenzione della corruzione e trasparenza e staff, autenticati tramite 2FA.

Il contratto disciplina:

- Istruzioni scritte del titolare: gestione tecnica, no elaborazione contenuti.
- Misure sicurezza: crittografia end-to-end, audit annuali ACN cloud.
- Sottotrattanti autorizzati: solo Transparency International.
- Durata: 12 mesi rinnovabile, eliminazione irreversibile dati a cessazione.
- Audit RPCT: diritto verifica conformità su richiesta.

Le nomine hanno valore contrattuale, sono sottoscritte, archiviate e disponibili per interessati (art.15 GDPR), garantendo accountability e conformità Linee Guida ANAC 478/2025.

Qualora il fornitore venisse cambiato, il Comune provvederà alla nomina ex art. 28 del nuovo fornitore, come parte integrante dei documenti contrattuali.

4.1.15.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.16 Sicurezza dei canali informatici

Il sistema di whistleblowing del Comune di Cagliari è gestito tramite una piattaforma cloud qualificata ACN SA-1721 Livello 1 (<https://comunecagliari.whistleblowing.it>). Il sistema è gestito senza infrastruttura on-premise, con migrazione completata dalla precedente installazione locale verso il cloud per migliorare sicurezza, resilienza, scalabilità e continuità operativa. Sono supportate segnalazioni orali tramite canali alternativi (telefonate, messaggistica vocale, incontri diretti), con verbalizzazione o registrazione su piattaforma crittografata previo consenso, e possibilità di anonimizzazione. Tali canali sono protetti da misure tecniche come cifratura, controllo accessi granulare e divieto di tracciamento non autorizzato, in conformità ai principi di privacy by design e by default (artt. 24, 25, 32 GDPR) e D.Lgs. 24/2023.

La piattaforma, basata su software open-source GlobalLeaks fornito dal progetto WhistleblowingIT di Whistleblowing Solutions e Transparency International Italia, garantisce la crittografia end-to-end dei dati in transito e at-rest, inclusi contenuti delle segnalazioni, identità del segnalante e allegati.

Per la gestione delle segnalazioni è utilizzato un questionario online strutturato con campi obbligatori e opzionali, accessibile in forma scritta, con ricezione limitata agli utenti autorizzati.

L'autenticazione avviene tramite credenziali istituzionali (nome, cognome, ruolo, telefono, email) e autenticazione a due fattori (2FA), con policy di data retention predefinita di 12 mesi e cancellazione automatica sicura.

4.1.16.1 Valutazione

VALUTAZIONE

ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.17 Controllo degli accessi fisici

L'accesso fisico alla piattaforma whistleblowing è garantito da una serie di accorgimenti e precauzioni atte a limitare e minimizzare la possibilità di un accesso non autorizzato, grazie alla natura cloud-based del sistema migrato ex PN, con dismissione completa dell'installazione on-premise precedente.

- La piattaforma è ospitata su infrastrutture cloud qualificate AgID (ACN) senza componenti hardware fisici locali residui; l'accesso avviene esclusivamente via web da postazioni autorizzate negli uffici comunali dedicati al RPCT.
- La sicurezza fisica è delegata al provider cloud certificato, con provider cloud certificato, con audit AgID; nessun armadio o apparecchiatura fisica locale è presente post-migrazione.

4.1.17.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.18 Sicurezza dell'hardware

Non sono presenti componenti di hardware fisici, la sicurezza del sistema di whistleblowing del Comune di Cagliari è garantita dalla migrazione completa a piattaforma cloud qualificata AgID (ACN), con dismissione totale dell'installazione on-premise precedente e assenza di componenti fisici locali.

4.1.18.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura accettabile sulla base delle finalità perseguite e modalità di trattamento.

4.1.19 Protezione contro fonti di rischio non umane

Non sono presenti componenti hardware fisici on-premise post-dismissione; la sicurezza è delegata al provider cloud.

4.1.19.1 Valutazione

VALUTAZIONE
NON APPLICABILE
COMMENTO DI VALUTAZIONE

4.1.20 Politica di tutela della privacy

Per attivare, gestire e mantenere nel tempo le misure di sicurezza, il Comune di Cagliari definisce le Linee guida per la tutela della privacy per i trattamenti effettuati nell'ambito del whistleblowing.

Alla data della presente valutazione è definito e formalizzato il Piano Triennale di Prevenzione della Corruzione e Trasparenza 2026-2028, la Procedura di gestione delle segnalazioni, l'informativa privacy sul trattamento dei dati personali, oltre alla formalizzazione delle responsabilità per i soggetti coinvolti: Titolare del trattamento (Comune di Cagliari), RPCT (Responsabile Prevenzione

Corruzione e Trasparenza), DPO (Responsabile Protezione Dati e provider come Responsabile Esterno del Trattamento.

Sono in corso aggiornamenti documentali per allineamento a D. Lgs. 24/2023, GDPR (privacy by design/default) e PTPC, nello specifico il Comune di Cagliari sta aggiornando le procedure per la gestione di un eventuale data breach, quella per l'esercizio dei diritti degli interessati e al contempo provvederà all'aggiornamento del registro dei trattamenti.

4.1.20.1 Valutazione

VALUTAZIONE
ACCETTABILE CON ELEMENTI DI MIGLIORAMENTO
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato. Finalizzare e condividere con il personale coinvolto la procedura per la gestione dei diritti degli interessati, la procedura per la gestione dei data breach, le linee guida e procedure predisposte in conformità alla Direttiva NIS2.

4.1.21 Gestione delle politiche di tutela della privacy

Il Comune di Cagliari ha strutturato un'organizzazione completa per la protezione dei dati personali legata al sistema whistleblowing, definendo con precisione ruoli e responsabilità nel rispetto delle normative privacy per gli enti locali.

L'organigramma privacy comprende: il Comune di Cagliari come Titolare del trattamento, la nomina del Responsabile per la protezione dei dati (DPO), il RPCT con il suo staff come gestore del canale di segnalazione, e la formalizzazione della nomina per Whistleblowing Solutions S.r.l. come Responsabile esterno del trattamento (art. 28 GDPR). Il registro dei trattamenti è mantenuto aggiornato regolarmente (art. 30 GDPR).

Il Comune di Cagliari ha inoltre aggiornato la procedura di gestione delle segnalazioni e l'informativa privacy in conformità normativa al D. Lgs. 24/2023 e Linee Guida ANAC n. 478/2025, per disciplinare la raccolta, il trattamento, la conservazione e la riservatezza delle segnalazioni.

Sono in elaborazione: analisi dei rischi DPIA, procedure data breach e gestione diritti interessati (tutti in bozza). La formazione privacy viene erogata regolarmente ai gestori del canale.

Sono in corso ulteriori aggiornamenti documentali per allineamento a D. Lgs. 24/2023 e alle Linee Guida ANAC n. 478/2025, nello specifico il Comune di Cagliari sta predisponendo la procedura per gestione di un eventuale data breach e la procedura da adottare in caso di richiesta di esercizio diritti da parte degli interessati.

4.1.21.1 Valutazione

VALUTAZIONE
ACCETTABILE CON ELEMENTI DI MIGLIORAMENTO
COMMENTO DI VALUTAZIONE
Misura di sicurezza parzialmente accettabile in relazione al trattamento effettuato. Formalizzare le nomine per le persone autorizzate che accedono ai dati raccolti tramite il sistema di gestione delle segnalazioni. Finalizzare e condividere con il personale coinvolto le procedure e linee guida del sistema di gestione privacy.

4.1.22 Gestione dei rischi

La presente DPIA rappresenta la valutazione formale dei rischi per il trattamento whistleblowing del Comune di Cagliari, adottando la metodologia standard a quattro fasi per l'analisi del rischio conforme al GDPR (art. 35):

- Definizione delle operazioni di trattamento e contesto (piattaforma GlobalLeaks, raccolta/gestione segnalazioni).
- Identificazione di minacce e vulnerabilità con valutazione probabilità di occorrenza.
- Valutazione dell'impatto sui diritti/libertà degli interessati.
- Calcolo del livello di rischio (probabilità × impatto) per prioritizzazione misure.

Sulla base dei risultati, il Comune attuerà azioni prioritarie di mitigazione per garantire il miglioramento continuo della sicurezza dei dati, in conformità a D. Lgs. 24/2023, Linee Guida ANAC 478/2025 e GDPR art. 32.

4.1.22.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Il presente documento rappresenta una prima attività evoluta di valutazione dei rischi specifica per il trattamento in questione

4.1.23 Integrare la protezione della privacy nei progetti

In piena attuazione dei principi privacy by design e privacy by default (art. 25 GDPR), il Comune di Cagliari ha integrato la tutela dei dati personali direttamente nella scelta della nuova piattaforma WhistleblowingIT basata su GlobaLeaks in sostituzione del precedente sistema di gestione delle segnalazioni.

La valutazione preliminare dei rischi è condotta dalla presente DPIA, che ha individuato l'adozione di soluzioni tecniche-organizzative per la minimizzazione del trattamento, a titolo esemplificativo e non esaustivo:

- Raccolta dati limitata alle segnalazioni essenziali.
- 2FA obbligatoria per tutti gli accessi autorizzati.
- Cifratura end-to-end nativa GlobaLeaks.
- Accesso granulare RBAC per ruoli definiti.

La nuova procedura di gestione delle segnalazioni e l'informativa privacy aggiornata, in conformità a D. Lgs. 24/2023, Linee Guida ANAC 478/2025 e GDPR, garantiscono massima trasparenza sulle finalità e modalità di trattamento.

4.1.23.1 Valutazione

VALUTAZIONE
ACCETTABILE CON ELEMENTI DI MIGLIORAMENTO

COMMENTO DI VALUTAZIONE

Formalizzare e applicare le linee guida per la Privacy by design/by default in modo strutturato nell'ambito dei processi legati al trattamento dei dati personali.

4.1.24 Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Il Comune di Cagliari, tra i vari aggiornamenti documentali, sta finalizzando la procedura per la gestione delle violazioni di dati personali, che includano le seguenti azioni:

- Il Titolare, previa consultazione del DPO, raccoglie e analizza gli eventi potenzialmente rischiosi per i dati personali in base ai risultati degli audit, segnalazioni o verifiche dirette.
- Qualora il Titolare valuti il Data Breach come potenzialmente rischioso, segnala alle Autorità competenti le violazioni entro 72 dalla conoscenza del fatto, tramite apposita procedura indicata dal Garante.
- Nel caso in cui non sia possibile notificare la violazione entro il suddetto limite di tempo, deve essere fornita adeguata spiegazione all'interno della notifica senza ulteriore ritardo.
- Il Titolare informa contestualmente gli interessati nel caso in cui la data breach possa determinare con buona probabilità un rischio per i diritti e le libertà fondamentali.
- Le violazioni dei dati personali sono registrate e gestite dal Titolare, con l'ausilio costante del DPO, attraverso il Registro degli incidenti.

4.1.24.1 Valutazione

VALUTAZIONE

ACCETTABILE CON ELEMENTI DI MIGLIORAMENTO

COMMENTO DI VALUTAZIONE

Misura di sicurezza accettabile in relazione al trattamento effettuato.

Finalizzare la procedura per la gestione di un eventuale data breach.

4.1.25 Gestione del personale

È individuato il personale che tratta dati personali del sistema whistleblowing del Comune di Cagliari: RPCT e staff (utenze registrate con ruolo gestione completa), sotto supervisione DPO.

Il Titolare, con la supervisione del DPO, deve garantire specifiche attività di sensibilizzazione e formazione per il personale autorizzato, sia all'ingresso in servizio che per cambiamenti mansioni o nuovi strumenti, come raccomandato dalle guide WBIT e obbligatorio ex art. 29/32 GDPR.

Tutto il personale deve essere istruito sul corretto trattamento dei dati personali whistleblowing (riservatezza, no ritorsioni, gestione segnalazioni); il Titolare pianifica interventi formativi periodici per i soggetti autorizzati, con registrazione evidenze, in linea con D. Lgs. 24/2023 e privacy by design.

4.1.25.1 Valutazione

VALUTAZIONE
ACCETTABILE CON ELEMENTI DI MIGLIORAMENTO
COMMENTO DI VALUTAZIONE
Rivedere ed eventualmente aggiornare le nomine alle persone che accedono al sistema di gestione delle segnalazioni come persone autorizzate al trattamento. Predisporre un documento di Istruzioni comportamentali e misure di sicurezza da consegnare alle persone autorizzate al trattamento. Pianificare e erogare periodicamente sessioni di formazione specifica a tutte le persone autorizzate.

4.1.26 Gestione dei terzi che accedono ai dati

La gestione e manutenzione tecnica del sistema whistleblowing del Comune di Cagliari – inclusi funzionamento, aggiornamenti e misure di sicurezza – è affidata al provider Whistleblowing Solutions , nominato come Responsabile Esterno del Trattamento ai sensi dell'art. 28 GDPR.

I sub-responsabili sono individuati in SEEWEB S.R.L. (archiviazione hosting cloud iass e backup), e TRANSPARENCY INTERNATIONAL ITALIA (supporto utenti amministratore di sistema)

Qualora il fornitore venisse cambiato, il Comune provvederà alla nomina ex art. 28 del nuovo fornitore, come parte integrante dei documenti contrattuali.

4.1.26.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato.

4.1.27 Vigilanza sulla protezione dei dati

Il Titolare del trattamento deve verificare costantemente che:

- vengano rispettati i diritti e le libertà fondamentali dei soggetti rispetto al trattamento effettuato;
- le politiche interne adottate siano allineate al principio di protezione dei dati dalla progettazione, al loro utilizzo;
- i dati siano protetti in tutto il loro ciclo di vita, dalla raccolta fino alla loro distruzione;
- i dati utilizzati siano sempre ridotti al minimo indispensabile per la finalità perseguita;
- i Responsabili del Trattamento siano correttamente istruiti sulle attività di trattamento da effettuare per proprio conto ne sia verificato l'operato.

Al fine di verificare la costante applicazione della normativa in materia di tutela dei dati personali, nonché delle linee guida definite, il Comune di Cagliari definisce, in accordo con il DPO, opportune attività di verifica.

Le attività di controllo e verifica possono avere come ambito i processi interni o potranno essere svolte anche nei confronti dei fornitori che trattino dati di cui il Comune di Cagliari sia titolare e siano stati nominati Responsabili esterni del trattamento. In tal caso le verifiche verteranno sulla corretta applicazione delle istruzioni impartite dal titolare e sulla costante applicazione delle misure di sicurezza necessarie a garantire la tutela dei dati personali trattati.

4.1.27.1 Valutazione

VALUTAZIONE
ACCETTABILE CON ELEMENTI DI MIGLIORAMENTO
COMMENTO DI VALUTAZIONE
Misura di sicurezza accettabile in relazione al trattamento effettuato. Mettere in atto il piano di verifica a fronte del quale provvedere all'aggiornamento periodico della presente DPIA.

4.2 Rischio di accesso illegittimo ai dati

4.2.1 Impatti potenziali sui soggetti interessati se il rischio si dovesse concretizzare

I principali impatti sui soggetti interessati in caso di concretizzazione del rischio di accesso illegittimo ai dati nel trattamento dei dati del sistema di whistleblowing del Comune di Cagliari sono i seguenti:

- a) Ritorsioni professionali gravi per il segnalante (demansionamento, trasferimento, licenziamento) e ritorsioni personali per il segnalato (danno reputazionale irreversibile nella comunità locale).
- b) Perdite economiche dirette (estinzione contratti fornitori/collaboratori basati su segnalazioni) e danni carrieristici (esclusione da gare d'appalto pubbliche).
- c) Traumi psicologici profondi per tutte le parti: segnalante esposto a ostracismo/mobilità interna, segnalato sottoposto a stigma pubblico, terzi menzionati danneggiati indirettamente.
- d) Compromissione della fiducia istituzionale nel sistema whistleblowing comunale, con inibizione futura delle segnalazioni e minor emersione di illeciti.
- e) Discriminazione basata su correlazione dati (profilazione reputazionale da contenuti segnalazioni aggregate).
- f) Perdita temporanea di controllo su dati estremamente sensibili (calunnie, accuse penali non verificate).
- g) Stress da notifica data breach con conseguenze reputazionali anche se non materialmente rilevanti.

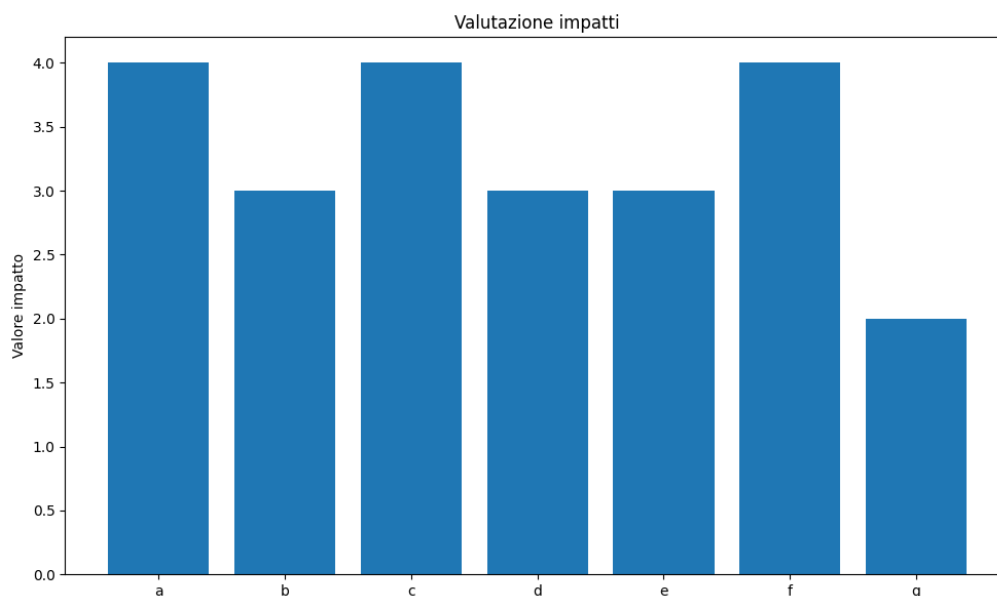
Questi impatti sono valutati considerando la particolare delicatezza delle informazioni trattate (accuse di corruzione/illeciti interni, art. 9-10 GDPR) e la posizione vulnerabile dei soggetti nel contesto lavorativo comunale.

Scala di valutazione dell'impatto

- 1 = Trascurabile
- 2 = Limitato
- 3 = Importante
- 4 = Grave

Tabella 1 – Valutazione degli impatti

Impatto	Descrizione sintetica	Valore
a	Ritorsioni professionali e personali	4
b	Perdite economiche e carrieristiche	3
c	Traumi psicologici	4
d	Compromissione fiducia istituzionale	3
e	Discriminazione / profilazione	3
f	Perdita controllo dati sensibili	4
g	Stress da data breach	2



4.2.2 Principali minacce che potrebbero concretizzare il rischio

- Accesso non autorizzato alla piattaforma da parte di utenti non autenticati o elevamento privilegi.
- Phishing/social engineering mirato per sottrazione credenziali 2FA.
- Intercettazione comunicazioni.
- Malware/ransomware su dispositivi per estrazione dati decifrati.
- Abuso autorizzazioni interne (accesso improprio da persone autorizzate che condividono contenuti).
- Violazione provider cloud (compromissione chiavi crittografiche o server).
- Errori configurazione piattaforma GlobalLeaks (credenziali deboli).
- Sociale engineering contro RPCT per accesso verbali canalizzazioni orali.
- Data retention leak (segnalazioni non cancellate dopo 12 mesi come da configurazione).
- Ingegneria sociale interna .

Scala di valutazione della probabilità

- 1 = Bassa
- 2 = Medio-bassa
- 3 = Media
- 4 = Alta

Tabella 2 – Probabilità intrinseca delle minacce

Minaccia	Probabilità (pre-mitigazione)
Accesso non autorizzato	3
Phishing/social engineering	4
Intercettazione comunicazioni	2
Malware/ransomware	3
Abuso autorizzazioni interne	3
Violazione provider cloud	2
Errori configurazione piattaforma	3
Social engineering contro RPCT	3
Data retention leak	2
Ingegneria sociale interna	3

4.2.3 Fonti di rischio

Fonte Umana interna

- Dipendenti (negligenti o malintenzionati);
- Collaboratori (negligenti o malintenzionati).

Fonte Umana Esterna

- Fornitori esterni.
- Terzi con o senza dolo.
- Hackers.

Fonti non Umane

- Virus Informatici.

4.2.4 Misure individuate che contribuiscono a mitigare il rischio

- Crittografia: Crittografia end-to-end per flussi in ingresso/uscita e a riposo (AES-256), HTTPS/TLS sicuro.

- Controllo degli accessi logici: Autenticazione 2FA obbligatoria.
- Tracciabilità: Log accessi piattaforma, registrazione eventi crittografati, audit interni con time-stamp.
- Archiviazione: Data retention 12 mesi automatica (estendibile fino a 5 anni) con cancellazione sicura.
- Contratto con il responsabile del trattamento: Nomina fornitore come Responsabile esterno art.28 GDPR, con clausole riservatezza e istruzioni.
- Gestione postazioni: Accesso solo da dispositivi autorizzati, nessuna infrastruttura locale (100% cloud PNRR ACN livello 1).
- Gestione vulnerabilità: Piattaforma Whistleblowing basata su GlobaLeaks open-source certificata ISO 27001 e cloud ACN livello 1.
- Lotta contro malware: Cloud PNRR qualificato ACN livello 1 con protezione anti-malware nativa, ISO 27001.
- Sicurezza siti web: HTTPS/TLS crittografato, piattaforma validata ANAC per enti pubblici
- Politica di tutela della privacy:
- Vigilanza sulla protezione dei dati.
- Gestione delle politiche di tutela della privacy: Sistema Gestione Privacy comunale, informative, sito web.
- Gestione dei rischi.
- Gestione del personale - Formazione persone autorizzate.
- Sicurezza dei canali informatici: HTTPS/TLS crittografato, piattaforma GlobaLeaks open-source validata ANAC.
- Minimizzazione dei dati.
- Manutenzione: Manutenzione gestita dal fornitore certificato ISO 27001.
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali: Procedure data breach (notifica Garante 72h), registro violazioni.

Scala di attenuazione (sulla probabilità)

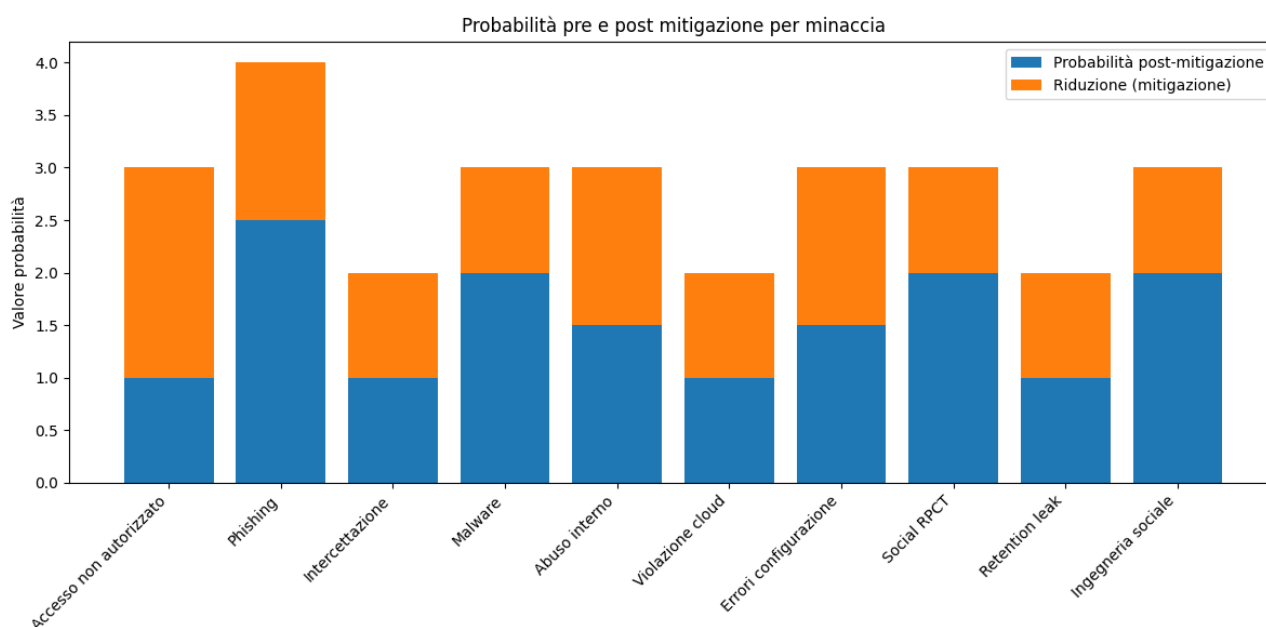
- 0,5 = riduzione lieve
- 1 = riduzione media
- 1,5 = riduzione significativa
- 2 = riduzione elevata

Tabella 3 – Probabilità post mitigazione

Minaccia	Probabilità iniziale	Attenuazione	Probabilità residua
Accesso non autorizzato	3	2	1
Phishing/social engineering	4	1,5	2,5
Intercettazione comunicazioni	2	1	1
Malware/ransomware	3	1	2

Abuso autorizzazioni interne	3	1,5	1,5
Violazione provider cloud	2	1	1
Errori configurazione piattaforma	3	1,5	1,5
Social engineering contro RPCT	3	1	2
Data retention leak	2	1	1
Ingegneria sociale interna	3	1	2

Rappresentazione grafica della probabilità



Il grafico a barre in pila rappresenta, per ciascuna minaccia:

- la **probabilità residua (post mitigazione)**
- la **riduzione della probabilità ottenuta tramite le misure**

la somma delle due componenti rappresenta la probabilità iniziale.

4.2.5 Gravità del rischio, riguardo i potenziali impatti e i controlli pianificati

Indefinito	Trascurabile	Limitato	Importante	Massimo
			X	

Gli interessati potrebbero sperimentare inconvenienti limitati a causa dell'accesso illegittimo ai dati e dalla conseguente perdita di riservatezza dei dati, superabili nonostante alcune difficoltà.

4.2.6 Probabilità del rischio, riguardo alle minacce, alle fonti di rischio e alle misure pianificate

Indefinito	Trascurabile	Limitato	Importante	Massimo
	X			

La probabilità è stata valutata considerando:

- valori iniziali delle minacce (2–4)
- riduzione derivante dalle misure (1–2 punti)

Il valore medio della probabilità residua è:

$$(1 + 2,5 + 1 + 2 + 1,5 + 1 + 1,5 + 2 + 1 + 2) / 10 = 1,65$$

Probabilità complessiva = TRASCURABILE

4.2.7 Valutazione complessiva

4.2.7.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE

La gravità è classificata come importante in ragione della natura dei dati trattati e dei possibili effetti sugli interessati.

La probabilità, inizialmente significativa per alcune minacce (in particolare phishing e social engineering), risulta ridotta grazie alle misure tecniche e organizzative implementate, come evidenziato nella riduzione dei valori di probabilità nelle tabelle e nel grafico.

Permangono livelli di attenzione sulle minacce legate al fattore umano, per le quali si raccomanda:

- monitoraggio continuo
- formazione periodica
- verifica delle misure

4.3 Rischio di modifiche indesiderate dei dati

4.3.1 Impatti potenziali sui soggetti interessati se il rischio si dovesse concretizzare

I principali impatti sui soggetti interessati in caso di concretizzazione del rischio di modifiche indesiderate ai dati nel trattamento dei dati del sistema di whistleblowing del Comune di Cagliari sono i seguenti:

- a) Errori nella ricostruzione degli illeciti (tempistiche, responsabilità, prove), con attribuzioni inesatte di colpa/innocenza a segnalante, segnalato o terzi menzionati.
- b) Inconvenienti procedurali gravi: avvio/disciplinari ingiustificati, denunce penali infondate, archiviazioni premature di segnalazioni fondate.
- c) Disagi relazionali permanenti nella comunità lavorativa comunale: segnalante percepito come "calunniatore", segnalato come "colpevole non accertato".
- d) Perdita affidabilità sistema whistleblowing: segnalanti futuri scoraggiati, illeciti non emersi, compromissione Piano Triennale Anticorruzione.
- e) Stress psicologico prolungato: incertezza su veridicità dati RPCT, paura ritorsioni basate su informazioni alterate.
- f) Ritardi indagini interne - necessità verifiche aggiuntive.
- g) Contestazioni/ricorsi multipli.
- h) Perdita fiducia istituzionale: cittadini/dipendenti percepiscono sistema manipolabile, inibizione segnalazioni future.

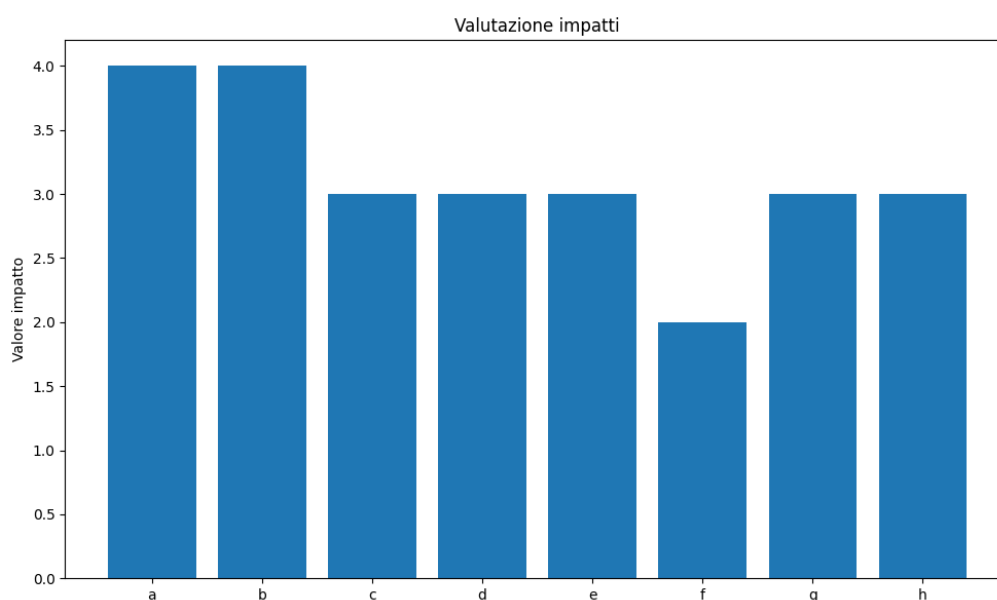
Tali impatti sono valutati considerando la massima delicatezza delle informazioni (accuse corruzione/illeciti interni, art. 9-10 GDPR) e posizione vulnerabile dei soggetti nel contesto lavorativo comunale, dove modifiche dati comprometterebbero irrevocabilmente reputazioni professionali.

Scala di valutazione dell'impatto

- 1 = Trascurabile
- 2 = Limitato
- 3 = Importante
- 4 = Grave

Tabella 1 – Valutazione degli impatti

Impatto	Descrizione sintetica	Valore
a	Errori nella ricostruzione degli illeciti e attribuzioni inesatte di responsabilità	4
b	Inconvenienti procedurali gravi e iniziative ingiustificate	4
c	Disagi relazionali permanenti nella comunità lavorativa	3
d	Perdita di affidabilità del sistema di whistleblowing	3
e	Stress psicologico prolungato dovuto a dati alterati	3
f	Ritardi nelle indagini interne e necessità di verifiche aggiuntive	2
g	Contestazioni e ricorsi multipli	3
h	Perdita di fiducia istituzionale e inibizione di segnalazioni future	3



4.3.2 Principali minacce che potrebbero consentire la concretizzazione del rischio

- Accesso non autorizzato alla piattaforma da parte di utenti non autenticati o elevamento privilegi.
- Phishing/social engineering mirato per sottrazione credenziali 2FA.
- Intercettazione comunicazioni.
- Malware/ransomware su dispositivi per estrazione dati decifrati.
- Abuso autorizzazioni interne (accesso improprio da persone autorizzate che condividono contenuti).
- Violazione provider cloud (compromissione chiavi crittografiche o server).
- Errori configurazione piattaforma GlobaLeaks (credenziali deboli).
- Sociale engineering contro RPCT per accesso verbali canalizzazioni orali.
- Data retention leak (segnalazioni non cancellate dopo 12 mesi come da configurazione).
- Ingegneria sociale interna.

Scala di valutazione della probabilità

- 1 = Bassa
- 2 = Medio-bassa
- 3 = Media
- 4 = Alta

Tabella 2 – Probabilità intrinseca delle minacce

Minaccia	Probabilità (pre-mitigazione)
Accesso non autorizzato alla piattaforma da parte di utenti non autenticati o elevamento privilegi	3
Phishing/social engineering mirato per sottrazione credenziali 2FA	4
Intercettazione comunicazioni	2
Malware/ransomware su dispositivi per estrazione dati decifrati	3
Abuso autorizzazioni interne (accesso improprio da persone autorizzate che condividono contenuti)	3
Violazione provider cloud (compromissione chiavi crittografiche o server)	2
Errori configurazione piattaforma GlobaLeaks (credenziali deboli)	3

Sociale engineering contro RPCT per accesso verbali canalizzazioni orali	3
Data retention leak (segnalazioni non cancellate dopo 12 mesi come da configurazione)	2
Ingegneria sociale interna	3

Le minacce sopra riportate presentano un livello di probabilità intrinseca medio o medio-alto, in quanto il sistema di whistleblowing, pur essendo supportato da una piattaforma specialistica, resta comunque esposto a minacce di natura tecnica, organizzativa e umana. Nel caso specifico del rischio di modifiche indesiderate dei dati, assumono particolare rilievo le minacce che possono consentire non solo l'accesso, ma anche l'alterazione dei contenuti, delle evidenze, delle tempistiche e dei metadati associati alla segnalazione.

4.3.3 Fonti di rischio

Fonte Umana interna

- Dipendenti (negligenti o malintenzionati);
- Collaboratori (negligenti o malintenzionati).

Fonte Umana Esterna

- Fornitori esterni.
- Terzi con o senza dolo.
- Hackers.

Fonti non Umane

- Virus Informatici.

4.3.4 Misure individuate che contribuiscono a mitigare il rischio

- Crittografia: Crittografia end-to-end per flussi in ingresso/uscita e a riposo (AES-256), HTTPS/TLS sicuro.
- Controllo degli accessi logici: Autenticazione 2FA obbligatoria.
- Tracciabilità: Log accessi piattaforma, registrazione eventi crittografati, audit interni con time-stamp.
- Archiviazione: Data retention 12 mesi automatica (estendibile fino a 5 anni) con cancellazione sicura.
- Contratto con il responsabile del trattamento: Nomina fornitore come Responsabile esterno art.28 GDPR, con clausole riservatezza e istruzioni.

- Gestione postazioni: Accesso solo da dispositivi autorizzati, nessuna infrastruttura locale (100% cloud PNRR ACN livello 1).
- Gestione vulnerabilità: Piattaforma Whistleblowing basata su GlobaLeaks open-source certificata ISO 27001 e cloud ACN livello 1.
- Lotta contro malware: Cloud PNRR qualificato ACN livello 1 con protezione anti-malware nativa, ISO 27001.
- Sicurezza siti web: HTTPS/TLS crittografato, piattaforma validata ANAC per enti pubblici
- Politica di tutela della privacy.
- Vigilanza sulla protezione dei dati.
- Gestione delle politiche di tutela della privacy: Sistema Gestione Privacy comunale, informative, sito web.
- Gestione dei rischi.
- Gestione del personale: Formazione persone autorizzate.
- Sicurezza dei canali informatici: HTTPS/TLS crittografato, piattaforma GlobaLeaks open-source validata ANAC.
- Minimizzazione dei dati.
- Manutenzione: Manutenzione gestita dal fornitore certificato ISO 27001.
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali: Procedure data breach (notifica Garante 72h), registro violazioni.

Scala di attenuazione (sulla probabilità)

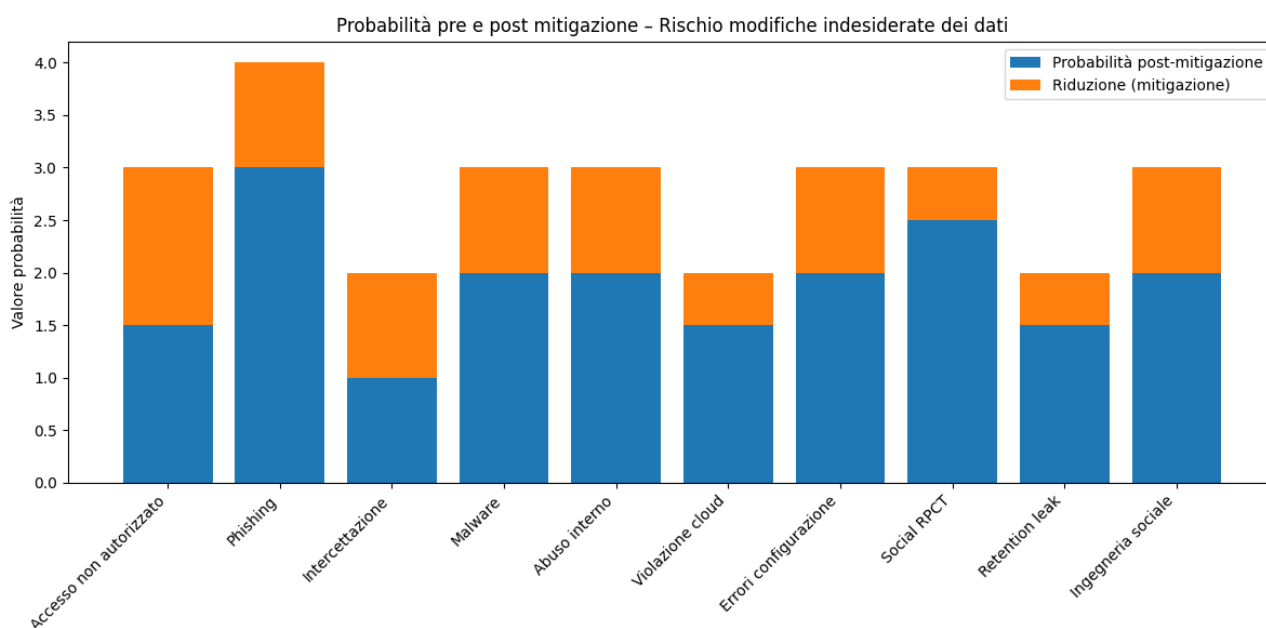
- 0,5 = riduzione lieve
- 1 = riduzione media
- 1,5 = riduzione significativa
- 2 = riduzione elevata

Tabella 3 – Probabilità post mitigazione

Minaccia	Probabilità iniziale	Attenuazione	Probabilità residua
Accesso non autorizzato alla piattaforma da parte di utenti non autenticati o elevamento privilegi	3	1,5	1,5
Phishing/social engineering mirato per sottrazione credenziali 2FA	4	1	3
Intercettazione comunicazioni	2	1	1
Malware/ransomware su dispositivi per estrazione dati decifrati	3	1	2
Abuso autorizzazioni interne (accesso improprio da persone autorizzate che condividono contenuti)	3	1	2
Violazione provider cloud (compromissione chiavi crittografiche o server)	2	0,5	1,5

Errori configurazione piattaforma GlobaLeaks (credenziali deboli)	3	1	2
Sociale engineering contro RPCT per accesso verbali canalizzazioni orali	3	0,5	2,5
Data retention leak (segnalazioni non cancellate dopo 12 mesi come da configurazione)	2	0,5	1,5
Ingegneria sociale interna	3	0,5	2,5

Rappresentazione grafica della probabilità



Il grafico a barre in pila rappresenta, per ciascuna minaccia:

- la **probabilità residua (post mitigazione)**;
- la **riduzione della probabilità ottenuta tramite le misure di mitigazione**.

La somma delle due componenti corrisponde alla **probabilità iniziale (pre mitigazione)**.

Nel caso del rischio di modifiche indesiderate dei dati, il grafico evidenzia una riduzione della probabilità meno marcata rispetto al rischio di accesso illegittimo, in quanto una parte delle misure disponibili agisce soprattutto sulla riservatezza, sulla tracciabilità o sulla rilevazione dell'evento, e solo parzialmente sulla prevenzione della modifica del dato.

4.3.5 Gravità del rischio riguardo ai potenziali impatti e alle misure pianificate

Indefinito	Trascurabile	Limitato	Importante	Massimo
			X	

Gli interessati potrebbero sperimentare conseguenze importanti a causa delle modifiche indesiderate dei dati.

La gravità è classificata come **IMPORTANTE** in quanto l'alterazione dei dati contenuti nella segnalazione può incidere in modo diretto sulla correttezza della ricostruzione dei fatti, sulla legittimità dei procedimenti conseguenti, sulla reputazione dei soggetti coinvolti e sulla affidabilità complessiva del sistema di whistleblowing in relazione alla tutela dei diritti degli interessati.

4.3.6 Probabilità del rischio riguardo minacce, fonti di rischio e controlli pianificati

Indefinito	Trascurabile	Limitato	Importante	Massimo
	X			

Sulla base delle misure di sicurezza adottate e dei dati statistici sugli incidenti occorsi, la probabilità che fonti di rischio umane o non umane effettuino delle modifiche indesiderate dei dati appare, ad oggi, trascurabile.

Ai fini della presente analisi numerica, la probabilità è stata valutata in termini di **probabilità residua media** delle minacce considerate, dopo l'applicazione delle attenuazioni derivanti dalle misure di mitigazione.

Il valore medio della probabilità residua è il seguente:

$$(1,5 + 3 + 1 + 2 + 2 + 1,5 + 2 + 2,5 + 1,5 + 2,5)/10 = 1,95$$

Il valore medio risultante (**1,95**) colloca la probabilità complessiva nella fascia **TRASCURABILE**.

Tale risultato è coerente con il fatto che le misure di sicurezza implementate riducono in maniera significativa il rischio di alterazione dei dati, ma non con la stessa intensità osservabile per i rischi che attengono esclusivamente alla riservatezza. Restano infatti maggiormente esposte le minacce con forte componente umana o connessa a uso legittimo ma scorretto delle credenziali e delle autorizzazioni, nonché le minacce in cui la modifica del dato può avvenire dall'interno del perimetro applicativo o organizzativo.

4.3.7 Valutazione complessiva

4.3.7.1 Valutazione

VALUTAZIONE
ACCETTABILE
COMMENTO DI VALUTAZIONE

La valutazione complessiva è ritenuta accettabile in quanto, pur in presenza di una gravità importante e di una probabilità residua classificabile come limitata, il sistema presenta un insieme strutturato di misure tecniche e organizzative idonee a ridurre in modo significativo la possibilità di alterazione dei dati.

La presenza di autenticazione forte, limitazione degli accessi, logging, audit trail, gestione specialistica della piattaforma, controllo degli endpoint, qualificazione del cloud e procedure organizzative dedicate consente di contenere il rischio entro una soglia accettabile.

4.4 Rischio di perdita di dati

4.4.1 Impatto sui soggetti interessati se il rischio dovesse realizzarsi

I principali impatti sui soggetti interessati in caso di concretizzazione del rischio di perdita di dati nel trattamento dei dati del sistema di whistleblowing del Comune di Cagliari sono i seguenti:

- i) Impossibilità di utilizzare segnalazioni/prove per tutelare diritti (segnalante non riceve riscontro, segnalato non contesta accuse).
- j) Esposizione a ritorsioni incontrollate: assenza prove archiviazioni premature, segnalato subisce stigma senza difesa documentale.
- k) Disagi prolungati in procedure: ritardi verifiche RPCT.
- l) Perdita fiducia irreversibile nel sistema whistleblowing RPCT, minor emersione futuri illeciti comunali.
- m) Compromissione tutele giudiziarie: perdita dati accuse corruzione preclude indagini penali/anticorruzione ANAC/Corte Conti, lasciando vittime senza giustizia.

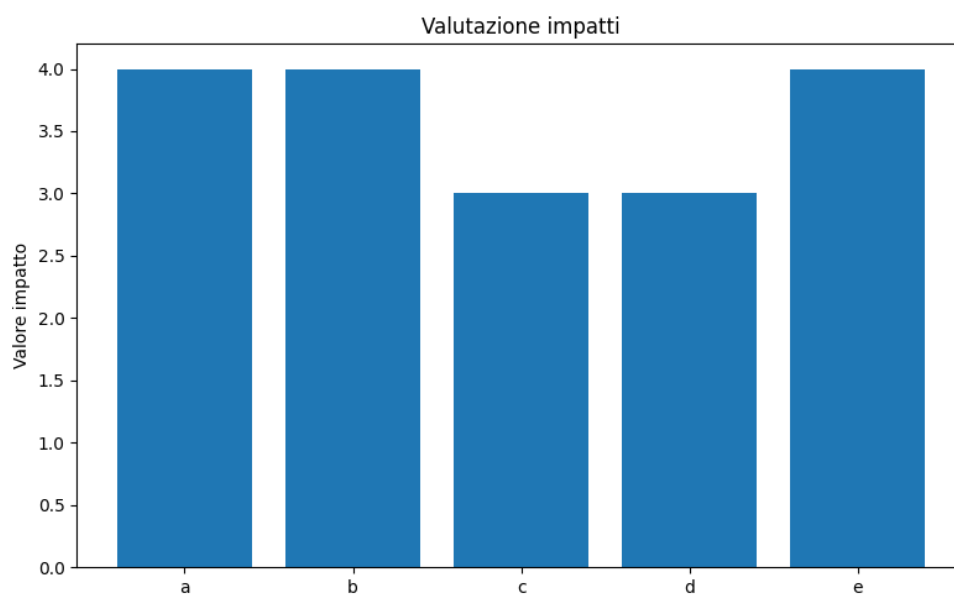
Scala di valutazione dell'impatto

- 1 = Trascurabile
- 2 = Limitato
- 3 = Importante
- 4 = Grave

Tabella 1 – Valutazione degli impatti

Impatto	Descrizione sintetica	Valore
---------	-----------------------	--------

a	Impossibilità di utilizzare prove e segnalazioni	4
b	Ritorsioni incontrollate per assenza evidenze	4
c	Ritardi procedurali e disagi operativi	3
d	Perdita fiducia nel sistema whistleblowing	3
e	Compromissione tutele giudiziarie	4



4.4.2 Principali minacce che potrebbero consentire la materializzazione del rischio

- Accesso non autorizzato alla piattaforma da parte di utenti non autenticati o elevamento privilegi.
- Phishing/social engineering mirato per sottrazione credenziali 2FA.
- Intercettazione comunicazioni.
- Malware/ransomware su dispositivi per estrazione dati decifrati.
- Abuso autorizzazioni interne (accesso improprio da persone autorizzate che condividono contenuti).
- Violazione provider cloud (compromissione chiavi crittografiche o server).
- Errori configurazione piattaforma GlobalLeaks (credenziali deboli).

- Sociale engineering contro RPCT per accesso verbali canalizzazioni orali.
- Data retention leak (segnalazioni non cancellate dopo 12 mesi come da configurazione).
- Ingegneria sociale interna.

Scala di valutazione della probabilità

- 1 = Bassa
- 2 = Medio-bassa
- 3 = Media
- 4 = Alta

Tabella 2 – Probabilità intrinseca delle minacce

Minaccia	Probabilità (pre-mitigazione)
Accesso non autorizzato	2
Phishing/social engineering	3
Intercettazione comunicazioni	2
Malware/ransomware	4
Abuso autorizzazioni interne	3
Violazione provider cloud	3
Errori configurazione piattaforma	3
Social engineering contro RPCT	2
Data retention leak	2
Ingegneria sociale interna	3

4.4.3 Fonti di rischio

Fonte Umana interna

- Dipendenti (negligenti o malintenzionati);
- Collaboratori (negligenti o malintenzionati).

Fonte Umana Esterna

- Fornitori esterni,
- Terzi con o senza dolo,

- Hackers.

Fonti non Umane

- Virus Informatici.

4.4.4 Misure fra quelle individuate che contribuiscono a mitigare il rischio

- Crittografia: Crittografia end-to-end per flussi in ingresso/uscita e a riposo (AES-256), HTTPS/TLS sicuro.
- Controllo degli accessi logici: Autenticazione 2FA obbligatoria.
- Tracciabilità: Log accessi piattaforma, registrazione eventi crittografati, audit interni con time-stamp.
- Archiviazione: Data retention 12 mesi automatica (estendibile fino a 5 anni) con cancellazione sicura.
- Contratto con il responsabile del trattamento - Nomina fornitore come Responsabile esterno art.28 GDPR, con clausole riservatezza e istruzioni.
- Gestione postazioni: Accesso solo da dispositivi autorizzati, nessuna infrastruttura locale (100% cloud PNRR ACN livello 1).
- Gestione vulnerabilità: Piattaforma Whistleblowing basata su GlobaLeaks open-source certificata ISO 27001 e cloud ACN livello 1.
- Lotta contro malware: Cloud PNRR qualificato ACN livello 1 con protezione anti-malware nativa, ISO 27001.
- Sicurezza siti web: HTTPS/TLS crittografato, piattaforma validata ANAC per enti pubblici
- Politica di tutela della privacy.
- Vigilanza sulla protezione dei dati.
- Gestione delle politiche di tutela della privacy: Sistema Gestione Privacy comunale, informative cartelli/sito web.
- Gestione dei rischi.
- Gestione del personale: Formazione persone autorizzate.
- Sicurezza dei canali informatici: HTTPS/TLS crittografato, piattaforma GlobaLeaks open-source validata ANAC.
- Minimizzazione dei dati.
- Manutenzione: Manutenzione gestita dal fornitore certificato ISO 27001.
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali: Procedure data breach (notifica Garante 72h), registro violazioni.

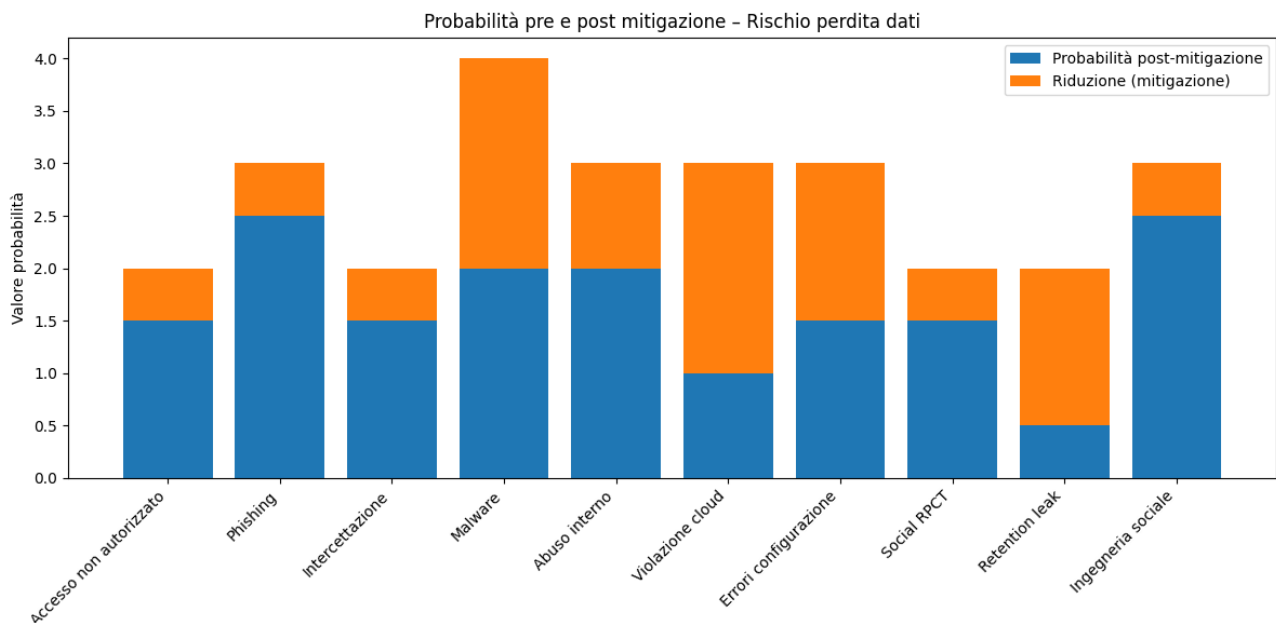
Scala di attenuazione

- 0,5 = bassa
- 1 = media
- 1,5 = significativa
- 2 = elevata

Tabella 3 – Probabilità post mitigazione

Minaccia	Probabilità iniziale	Attenuazione	Probabilità residua
Accesso non autorizzato	2	0,5	1,5
Phishing/social engineering	3	0,5	2,5
Intercettazione comunicazioni	2	0,5	1,5
Malware/ransomware	4	2	2
Abuso autorizzazioni interne	3	1	2
Violazione provider cloud	3	2	1
Errori configurazione piattaforma	3	1,5	1,5
Social engineering contro RPCT	2	0,5	1,5
Data retention leak	2	1,5	0,5
Ingegneria sociale interna	3	0,5	2,5

Rappresentazione grafica della probabilità



Il grafico a barre in pila rappresenta, per ciascuna minaccia:

- la probabilità residua (parte inferiore della barra)
- la riduzione ottenuta grazie alle misure di mitigazione (parte superiore della barra)

La somma delle due componenti corrisponde alla probabilità iniziale.

Dal grafico emerge che:

- la riduzione è **molto significativa** per minacce tecniche (malware, cloud)
- la riduzione è **limitata** per minacce umane (phishing, ingegneria sociale)

4.4.5 Gravità del rischio, in relazione degli impatti potenziali e delle misure pianificate

Indefinito	Trascurabile	Limitato	Importante	Massimo
			X	

Gli interessati potrebbero subire gravi conseguenze dalla perdita dei dati, in alcuni casi superabili con difficoltà.

4.4.6 Probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate

Indefinito	Trascurabile	Limitato	Importante	Massimo
		X		

Le misure di sicurezza applicate e i dati statistici sugli incidenti consentono di valutare come limitate le probabilità di perdita dei dati.

4.4.7 Valutazione complessiva

4.4.7.1 Valutazione

VALUTAZIONE
ACCETTABILE CON AZIONI DI MIGLIORAMENTO
COMMENTO DI VALUTAZIONE
Valutazione accettabile con azioni di miglioramento. Il rischio presenta una gravità importante in quanto la perdita dei dati può compromettere la tutela dei diritti degli interessati e l'efficacia del sistema di whistleblowing. La probabilità risulta limitata grazie alle misure implementate, in particolare quelle relative a infrastruttura cloud, protezione malware e gestione tecnica della piattaforma. Permangono criticità legate al fattore umano e alla gestione operativa, che richiedono monitoraggio continuo, formazione e miglioramento delle misure organizzative.

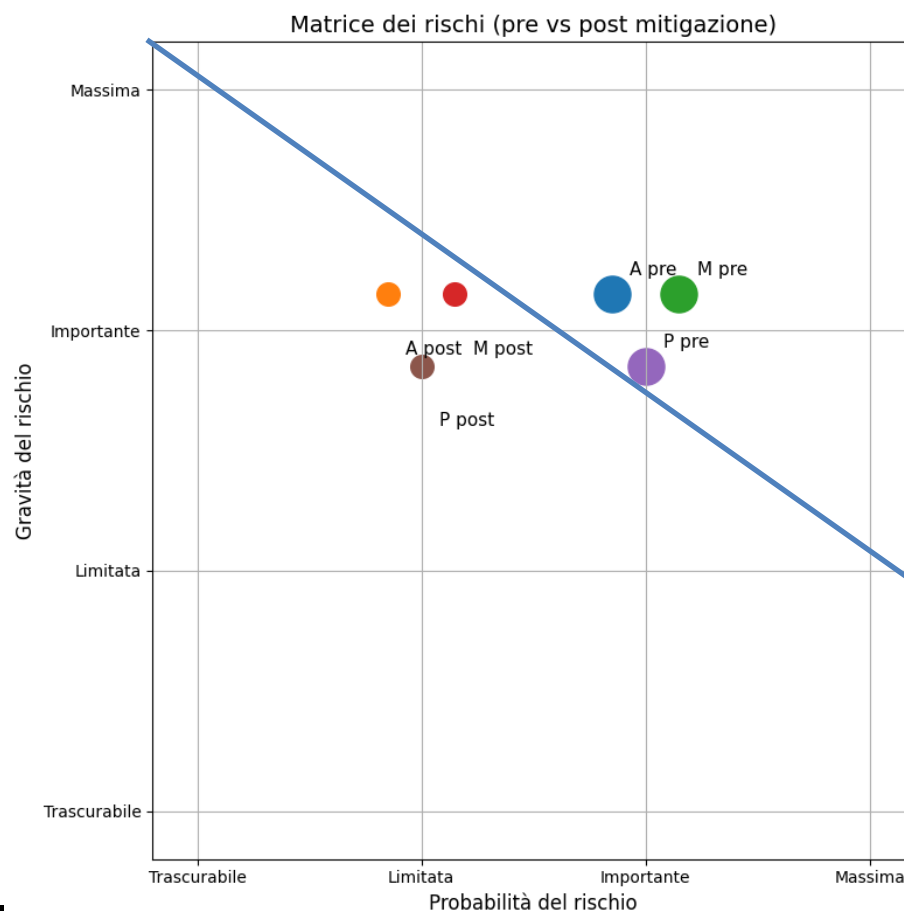
5 Convalida

Si rappresenta di seguito la mappa del rischio residuo, quale risultato dell'Assessment condotto e delle misure di sicurezza tecniche e organizzative in atto e pianificate, descritte sinteticamente nel successivo paragrafo 5.2.

Il risultato finale è di Rischio non elevato in considerazione delle misure di sicurezza applicate.

Tale documento di DPIA sarà aggiornato sulla base di rilevanti cambiamenti di carattere normativo, organizzativo e tecnologico.

5.1 Mappatura del rischio



Legenda:

A: Rischio connesso all'accesso illegittimo ai dati

M: Rischio connesso a modifiche indesiderate dei dati

P: Rischio connesso alla perdita dei dati

5.2 Piano d'azione

5.2.1 Misure di rimedio e di miglioramento

Si riportano di seguito le misure di rimedio e di miglioramento classificate per macro categoria di conformità normativa e sicurezza.

Per tali azioni sarà effettuata una valutazione in merito alle tempistiche di realizzazione, anche in considerazione della loro efficacia e del costo da sostenere.

Integrare la protezione della privacy nei progetti

- Applicare le linee guida per la privacy by design/by default in modo strutturato nell'ambito dei processi legati al trattamento dei dati personali.

Gestione del personale

- Nominare formalmente tutte le persone che gestiscono il canale di segnalazione come persone autorizzate al trattamento dei dati.
- Formalizzare e condividere internamente una Policy / documento di Istruzioni comportamentali per le persone autorizzate al trattamento.
- Completare le attività di sensibilizzazione e formazione per il personale coinvolto nei trattamenti di dati personali, prevedendo un piano di formazione annuale con obiettivi definiti.
- Assicurare che, in caso di riorganizzazioni o cessazioni, vi sia una procedura chiara per revocare tempestivamente diritti, responsabilità e profili di autorizzazione, con contestuale riconsegna di materiali e mezzi.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

- Finalizzare la procedura di gestione delle violazioni (data breach).
- Condividere la procedura con tutto il personale coinvolto.
- Pianificare e erogare specifiche sessioni di formazione a tutto il personale autorizzato.

Gestire dei diritti degli interessati

- Finalizzare la procedura di gestione dei diritti degli interessati.
- Condividere la procedura con tutto il personale coinvolto.
- Pianificare e erogare specifiche sessioni di formazione a tutto il personale autorizzato.

Gestire sicurezza delle forniture

- Finalizzare il framework documentale per la compliance dei servizi di fornitura, per i quali vi sia un accesso di terze parti ai dati personali.
- Pianificare ed eseguire attività di audit sui fornitori che accedono ai dati personali di cui il Comune di Cagliari è titolare.

Controllo degli accessi

- Individuare e nominare formalmente tutte le persone che accedono al canale di segnalazione.
- Formalizzare e condividere internamente una Policy / documento di Istruzioni comportamentali per le persone autorizzate al trattamento.

5.2.3 Nome del DPO e parere

Avv.. Giovanni Battista Gallus - Ha preso visione del documento ed espresso il seguente parere:.

La DPIA risulta, nel suo impianto complessivo, strutturata in modo conforme alla metodologia raccomandata dal CNIL e coerente con gli standard internazionali. Il documento affronta in modo sistematico il contesto del trattamento, l'individuazione delle basi giuridiche, le categorie di dati trattati, il ciclo di vita dei dati, le misure tecniche e organizzative adottate, nonché l'analisi dei rischi di accesso illegittimo, modifiche indesiderate e perdita dei dati.

La scelta della piattaforma WhistleblowingIT basata su GlobaLeaks, in configurazione cloud qualificato ACN, appare adeguata sotto il profilo delle garanzie di sicurezza (crittografia end-to-end, AES-256 at-rest, 2FA obbligatoria, separazione logica multi-tenant, cancellazione automatica programmata). La migrazione dall'infrastruttura on-premise precedente al cloud certificato costituisce un elemento positivo in termini di resilienza, continuità operativa e conformità alle prescrizioni del D.Lgs. 24/2023.

Dall'esame della documentazione emerge, in primo luogo, che il trattamento è legittimo e necessario, in quanto funzionale all'adempimento di obblighi normativi e alla tutela dell'interesse pubblico all'integrità amministrativa; la stessa DPIA indica, correttamente, che il trattamento non è fondato sul consenso, ma su obbligo legale e compito di interesse pubblico. Il trattamento in esame si colloca nel quadro della disciplina nazionale sul whistleblowing e delle Linee guida ANAC sui canali interni di segnalazione, approvate con delibera n. 478 del 26 novembre 2025.

La stessa DPIA, peraltro, dà atto che diverse misure organizzative e documentali risultano ancora da completare, tra cui la procedura di gestione delle violazioni di dati personali, la procedura di

gestione dei diritti degli interessati, la formalizzazione delle autorizzazioni, le istruzioni comportamentali, la formazione del personale e gli audit sui fornitori.

Con riguardo al canale orale, la documentazione richiama l'incontro con il RPCT e, nella DPIA, il recapito PEC del Segretario generale/RPCT quale modalità di esercizio di istanze e contatti. ANAC ha chiarito che, tra i canali utilizzabili, può esservi anche un indirizzo di posta elettronica, purché sia visibile al solo RPCT e assistito da adeguati accorgimenti di riservatezza. Su questo punto è opportuno che l'atto organizzativo e l'informativa precisino espressamente la natura dedicata e riservata del recapito utilizzato, oppure si individui un altro canale che garantisca la necessaria riservatezza.

Da ultimo, occorre uniformare le modalità di contatto per l'esercizio dei diritti, tra quanto indicato nell'informativa e nella DPIA.

Il DPO pertanto esprime parere favorevole, con la raccomandazione di adottare nel più breve tempo possibile le azioni di miglioramento già indicate nella stessa DPIA.

5.2.4 Richiesta del parere degli interessati.

Non è stato richiesto il parere degli interessati, considerato che non si rilevano i presupposti di obbligatorietà (Rischio non elevato).

L'attivazione e le modifiche sostanziali del canale interno di segnalazione sono effettuate previo coinvolgimento delle rappresentanze o organizzazioni sindacali (RSU/RSA) comparativamente più rappresentative sul piano nazionale, ai sensi dell'art. 4, co. 1, del D.Lgs. n. 24/2023. Tale coinvolgimento ha carattere meramente informativo e consente all'Ente di acquisire le eventuali osservazioni di parte sindacale sull'implementazione del canale interno. Il parere espresso dai sindacati nell'interlocuzione preventiva non ha natura vincolante.

6. Documentazione

1. **Piano per la prevenzione della corruzione e della trasparenza 2026-2028**
(<https://www.comune.cagliari.it/portale/page/it/piaoanno?contentId=STR251321>)
2. **Procedura di segnalazione Whistleblowing**
Procedura di gestione delle segnalazioni, disponibile nella pagina dedicata del portale istituzionale
(https://www.comune.cagliari.it/portale/page/it/dettaglio_prevenzione_corruzione?contentId=STR64760)
3. **Informativa privacy Whistleblowing**
Informativa tra Ente e segnalante disponibile nella pagina dedicata del portale istituzionale
(https://www.comune.cagliari.it/portale/page/it/dettaglio_prevenzione_corruzione?contentId=STR64760)

4. Documentazione WhistleblowingIT

Documentazione a supporto del titolare nella valutazione d'impatto sulla protezione dei dati
(<https://whistleblowing.it/documentazione-tecnica/>)



RICCARDO
CASTRIGNANÒ
02.07.2026
12:44:45
GMT+02:00

