Data Privacy Impact Assessment (DPIA)

Whistleblowing – segnalazione tramite incontro diretto

Unione Montana dei Comuni del Mugello

1. Premessa

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito "GDPR"), ogni qualvolta si debba iniziare un trattamento che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è necessario predisporre una DPIA, in particolare se il trattamento è connesso all'impiego di nuove tecnologie.

La DPIA (Data Protection Impact Assessment) corrisponde alla valutazione d'impatto del trattamento dei dati personali. Si dovranno considerare la natura, il contesto e le finalità del trattamento ed i rischi collegati.

La DPIA consente al Titolare del trattamento di prendere visione del rischio prima di procedere al trattamento in modo da annullare o quantomeno ridurre fortemente i rischi connessi al trattamento.

Il rischio residuo dovrà essere valutato in funzione della finalità e del diritto/dovere in capo al Titolare di eseguire tale trattamento.

I principi fondamentali della DPIA risultano pertanto:
- i diritti e le libertà fondamentali dell'interessato, punto fondante dell'intero impianto del GDPR;
- i trattamenti dei dati personali attraverso l'analisi della tipologia dei dati, gli strumenti che si intende utilizzare, le procedure e l'organizzazione del lavoro.
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio sia digitale che analogico (sicurezza fisica del dato elettronico, del dato cartaceo e di ogni contenitore dei dati elettronici e cartacei).

2. Contesto

2.1. Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni e dei soggetti segnalati ai sensi del D.lgs. n. 24/2023.

Modalità utilizzata: canale interno – incontro diretto su richiesta del Segnalante

Il Segnalante può richiedere un appuntamento con la persona delegata alla gestione delle segnalazioni, se il Segnalante acconsente sarà possibile verbalizzare l'incontro.

2.2 Organizzazione

Il Segnalante può contattare la persona delegata alla gestione delle segnalazioni (Responsabile RPCT).

L'appuntamento potrà essere fissato nel luogo che l'RPCT riterrà più funzionale alla raccolta delle informazioni e alla tutela della riservatezza delle stesse, del Segnalante e delle altre persone coinvolte.

L'eventuale verbale, le evidenze consegnate dal Segnalante e gli appunti dell'RPCT saranno conservati in locale chiuso a chiave e non dovranno essere accessibili a persone non autorizzate.

2.3 Responsabilità connesse al trattamento

Ruolo	Nominativo
Titolare del trattamento	UNIONE MONTANA DEI COMUNI DEL MUGELLO
Delegato al trattamento	Responsabile della prevenzione della corruzione e della trasparenza (RPCT)

2.4 Standard applicabili al trattamento

Al trattamento in materia di segnalazioni e normativa whistleblowing si applicano le seguenti normative e standard.

Regolamento UE n. 2016/679 (c.d. GDPR)

D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018

Direttiva UE 1937/2019

D.lgs. n. 24/2023

2.5 Dati personali e Interessati

Di seguito si riportano le tipologie di dati personali che sono oggetto di trattamento a seguito di una segnalazione fatta ai sensi del D.lgs. n. 24/2023

Categoria di dato personale Categoria di interessato

I dati personali potranno riguardare Dipendenti, Collaboratori e Fornitori che effettuano una segnalazione o che ne sono oggetto.

Dati personali comuni (es. dati di contatto).

Dati personali particolari (es. dati relativi alla salute, condanne penali)

2.6 Rischi per gli interessati

La mancata protezione dei dati personali delle persone coinvolte nella segnalazione (segnalante, segnalato, facilitatore ed altre persone previste per legame parentale o affettivo al segnalante) può comportare conseguenze personali come ritorsioni, giudizi sommari, discriminazioni.

3. Principi Fondamentali

Gli scopi del trattamento sono specifici, espliciti e legittimi

Il trattamento è finalizzato esclusivamente alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing.

Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui è tenuto il titolare (GDPR 679/2016 art. 6.1. lett. c). Riguardo a talune comunicazioni riguardanti il segnalante, potrebbe essere necessario il consenso per procedere a specifici trattamenti.

I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D.lgs. n. 24/2023. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (GDPR 679/2016 art. 5.1. lett. c).

I dati personali relativi alla segnalazione possono essere comuni e particolari e vengono ritenuti indispensabili dal segnalante in fase di segnalazione o dalla persona incaricata dal Titolare in fase di verifica della segnalazione.

I dati personali relativi alle segnalazioni sono costantemente aggiornati e integrati da parte della persona incaricata della gestione delle segnalazioni e possono essere aggiornati e integrati dal segnalante.

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e per ulteriore periodo necessario a poter provare di aver adempiuto agli obblighi di legge.

Il trattamento è sempre preceduto da informativa come meglio indicato al punto 3.1.

Il periodo di conservazione non potrà essere superiore a cinque anni.

3.1. Misure a tutela dei diritti degli interessati

Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR 679/2016.

L'informativa viene resa disponibile secondo le seguenti modalità:

- Affissione negli uffici

- Pubblicazione sito internet – sezione dedicata al Whistleblowing

Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (Art. 6.1. lett. c) del GDPR).

Nel caso invece ricorra l'ipotesi di comunicazione dei dati personali a soggetti diversi da quelli espressamente autorizzati dal Titolare, il segnalante dovrà prestare il proprio consenso.

Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR 679/2016 attraverso i canali di comunicazione indicati nell'informativa.

La persona delegata alla gestione delle segnalazioni è stata nominata in forma scritta.

Per questa tipologia di trattamento non è previsto un trasferimento di dati personali fuori dall'Unione Europea.

4. Misure esistenti

La persona delegata alla gestione delle segnalazioni è stata istruita riguardo al trattamento dei dati.

Le informazioni relative alle segnalazioni, eventuali appunti e altre informazioni che dovesse raccogliere durante la verifica dovranno essere conservate in ambiente chiuso e non accessibile da parte di altre persone.

La conservazione delle informazioni risulta essere più sicura se conservata su piattaforma web (vedere DPIA relativa) rispetto a supporto cartaceo, sia per quanto riguarda la sicurezza fisica rispetto ad accessi non autorizzati, sia per quanto riguarda il rischio di distruzione.

Per quanto sopra esposto risulta opportuno indirizzare il Segnalante all'utilizzo della piattaforma web, se questo non fosse possibile per legittima scelta dello stesso segnalante si procederà con l'incontro diretto.

Durante le verifiche la persona delegata alla gestione delle segnalazioni potrà relazionarsi con personale di altri uffici, in queste occasioni dovrà comunicare i soli dati necessari alla verifica. In nessun caso dovrà comunicare il nominativo del Segnalante.

5. Rischi

I rischi per i dati personali sono

- Accesso non autorizzato / Perdita di riservatezza
- Perdita dei dati

5.1 Accesso non autorizzato

La conservazione in luogo chiuso e non accessibile a persone non autorizzate impedisce, in molti casi, l'accesso ai dati.

Dovrà essere prestata la massima attenzione anche nella custodia delle chiavi necessarie per accedere ai dati.

Considerando che in passato gli eventi qui descritti (accesso non autorizzato in ambienti chiusi a chiave) non si sono verificati, si ritiene poco probabile che questo rischio possa concretizzarsi in futuro.

5.2 Violazione dei dati

La violazione dei dati può avvenire a seguito di:

- accesso da parte di persone non autorizzate;
- eventi esterni (es. incendio, terremoto).

5.2.1 Accesso non autorizzato

Persone non autorizzate potrebbero venire in contatto con dati personali relativi alle segnalazioni nel caso in cui:

- la persona delegata alla gestione delle segnalazioni dovesse lasciare incustodite le chiavi;
- dovesse verificarsi un caso di effrazione.

La persona delegata alla gestione delle segnalazioni è consapevole dell'importanza di riservatezza dei dati relativi ad una segnalazione e, considerando anche il ruolo che ricopre, si ritiene che il rischio di commettere una leggerezza nella custodia delle chiavi sia molto basso.

Considerando la storia dell'Ente non si rilevano casi di effrazione o furti di dati. E' installato un sistema di videosorveglianza e nel caso in cui qualcuno tentasse di forzare una serratura per entrare nella sede verrebbe ripreso. Nel caso in cui dovesse avvenire durante l'orario di lavoro, dovrebbe comunque forzare la serratura dell'ufficio (quando l'ufficio non è presidiato è chiuso. Il rischio di accesso non autorizzato a seguito di effrazione è da considerarsi basso.

5.2.3 Evento esterno

Eventi esterni come un incendio o un terremoto, per quanto improbabili, si possono verificare e i danni potrebbero causare la perdita di riservatezza delle informazioni oppure la distruzione delle stesse.

La perdita di riservatezza delle informazioni non è superabile in caso di eventi esterni estremi. Per quanto riguarda la distruzione, si potrebbe pensare a copie dei documenti da conservare in altro luogo ma questa soluzione andrebbe ad aumentare il rischio di accesso non autorizzato.

Considerando i diversi rischi si ritiene più sicuro evitare copie dei documenti.

Il rischio da evento esterno risulta essere maggiormente mitigato nella gestione delle segnalazioni attraverso piattaforma web.

6. Parere delle parti interessate

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge. Ai fini dell'attivazione del canale di segnalazione interna, gli enti devono sentire le rappresentanze o le organizzazioni sindacali.

7. Parere DPO

Il DPO esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo.

8. Conclusioni

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono rischi residui con impatto sui diritti e libertà degli interessati con stima a valore basso.

Considerando le attività di mitigazione dei rischi messe in atto dal Titolare si ritiene che i rischi del trattamento preso in considerazione siano da considerarsi bassi.

Considerando che il trattamento è obbligatorio e che il grado di rischio sui diritti e libertà dell'interessato è basso, si ritiene non necessaria una consultazione preventiva all'Autorità Garante.

Si potrà quindi procedere con il trattamento a condizione di rivalutare la presente DPIA ogni qualvolta dovesse modificare una o più informazioni che la riguardano e comunque almeno una volta all'anno per controllare che non siano intervenute modifiche alla presente analisi.

Borgo San Lorenzo, lì _____

_____