DPIA Whistleblowing

Comune di Vittoria

Vers. 1.0

21/03/2025

CITTÀ DI VITTORIA

Sommario

1. Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), la DPIA corrisponde alla valutazione d'impatto del trattamento del dato sulla protezione dei dati personali, qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ciò considerata la natura, il contesto e le finalità del trattamento.

Il GDPR introduce dunque una valutazione di stampo preliminare, che consente al Titolare del trattamento di prendere visione del rischio prima ancora di procedere al trattamento e di attivarsi perché tale rischio possa essere, se non annullato, quantomeno fortemente ridotto.

I principi fondamentali della DPIA risultano pertanto:

- i diritti e le libertà fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR;
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio.

Una DPIA poggia su due pilastri:

1. i principi e i diritti fondamentali, i quali sono "non negoziabili", stabiliti dalla legge e che devono essere rispettati e non possono essere soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi;
2. la gestione dei rischi per la privacy dei soggetti interessati, che determina i controlli tecnici e organizzativi opportuni a tutela dei dati personali.

La Metodologia di analisi dei rischi adottata nella conduzione delle attività di Data Privacy Impact Assessment è la metodologia di analisi CNIL del Garante Francese (o altra metodologia definita dal Titolare del trattamento), metodologia riconosciuta e approvata dal Garante della Privacy italiana.

Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento: Comune di Vittoria
Responsabile del trattamento: Whistleblowing Solutions I.S. S.r.l.

Ci sono 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.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

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:

- Dati personali comuni e di contatto

- Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto;
- Fornitori, subfornitori e dipendenti e collaboratori degli stessi che effettuano una segnalazione o vengono segnalati;
- Liberi professionisti, consulenti, lavoratori autonomi che effettuano una segnalazione o che ne sono oggetto;
- Volontari e tirocinanti, retribuiti o non retribuiti che effettuano una segnalazione o che ne sono oggetto;
- Azionisti o persone con funzione di amministrazione, direzione, vigilanza, controllo o rappresentanza che effettuano una segnalazione o che ne sono oggetto.

- Dati personali particolari (es. dati relativi alla salute, dati relativi all'appartenenza sindacale):

- Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto;
- Fornitori, subfornitori e dipendenti e collaboratori degli stessi che effettuano una segnalazione o vengono segnalati;
- Liberi professionisti, consulenti, lavoratori autonomi che effettuano una segnalazione o che ne sono oggetto;
- Volontari e tirocinanti, retribuiti o non retribuiti che effettuano una segnalazione o che ne sono oggetto;
- Azionisti o persone con funzione di amministrazione, direzione, vigilanza, controllo o rappresentanza che effettuano una segnalazione o che ne sono oggetto.

- Dati giudiziari (es. condanne penali):

- Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto;
- Fornitori, subfornitori e dipendenti e collaboratori degli stessi che effettuano una segnalazione o vengono segnalati;
- Liberi professionisti, consulenti, lavoratori autonomi che effettuano una segnalazione o che ne sono oggetto;
- Volontari e tirocinanti, retribuiti o non retribuiti che effettuano una segnalazione o che ne sono oggetto;
- Azionisti o persone con funzione di amministrazione, direzione, vigilanza, controllo o rappresentanza che effettuano una segnalazione o che ne sono oggetto.

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

1. Attivazione e configurazione della piattaforma;
2. Utilizzo della piattaforma – invio delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei soggetti autorizzati;

3. Dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.

Quali sono le risorse di supporto ai dati?

Piattaforma Web WhistleblowingIT

2. Principi Fondamentali

Proporzionalità e necessità

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.

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui è tenuto il titolare (Art. 6.1. lett. c) del GDPR).

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

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 (art. 5.1. lett. c) GDPR).

I dati sono esatti e aggiornati?

Il trattamento dei dati personali relativi alle segnalazioni sono costantemente aggiornati, poichè i soggetti incaricati di ricevere e gestire le segnalazioni ne verificano preliminarmente la corrispondenza a verità.

Qual è il periodo di conservazione dei dati?

Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 14/2023.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

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

L'informativa viene resa disponibile secondo le seguenti modalità:

- Processo comunicazione aziendale sull'esistenza del canale di segnalazione interno (canale informatico);
- Pubblicazione sito internet – sezione dedicata al Whistleblowing.
-

Ove applicabile: come si ottiene il consenso degli interessati?

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 suo consenso specifico alla segnalazione, tramite piattaforma, ai sensi degli artt. 6.1. lett. a) e 7 del GDPR.

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

Gli interessati possono esercitare i diritti previsti dagli artt. 15 e ss. del GDPR attraverso l'indirizzo di posta elettronica: dpo@comunevittoria-rg.it o contattando direttamente il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), nei limiti di cui all'articolo 2-undecies del Codice Privacy.

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

Il diritto all'oblio si realizza automaticamente entro i termini previsti dalla norma per cui i dati sono conservati per cinque anni e comunque per tutta la durata dell'eventuale procedimento disciplinare.

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

I dati inseriti nella segnalazione sono già limitati e pertinenti alla liceità del trattamento previsto, allo scopo di svolgere correttamente i principi di privacy della segnalazione stessa. In qualsiasi momento, gli interessati possono esercitare i diritti previsti dagli artt. 15 e ss. del GDPR attraverso l'indirizzo di posta elettronica: dpo@comunevittoria-rg.it o contattando direttamente il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), nei limiti di cui all'articolo 2-undecies del Codice Privacy.

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

Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del trattamento ai sensi dell'art. 28 GDPR, attraverso contratti o altri atti giuridici.

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

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

3. Rischi

Misure esistenti o pianificate

Crittografia e Sicurezza Canali Informatici

Ogni informazione viene protetta in transito da supporto HTTPS con protocollo TLS 1.3 standard e punteggio A+ in SSLabs.

Controllo degli accessi logici

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.

Tracciabilità

Viene utilizzato un meccanismo che memorizza un identificativo dell'operatore autorizzato e la data/ora di creazione o modifica delle informazioni presenti nel database.

Le operazioni effettuate dai segnalanti hanno un identificativo anonimizzato (autogenerato) e legato al singolo ticket e non alla persona del segnalante.

Archiviazione

L'applicativo ha completo ed esclusivo controllo della base dati ed implementa al suo interno le logiche di data retention e cancellazione sicura previste dalle policy normative.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Il prodotto è conforme con le normative GDPR in materia di gestione delle politiche di tutela ella privacy.

Gli amministratori e gli sviluppatori del prodotto operano in contesti di sicurezza conformi alle linee guida in materia, con firewall e antivirus aziendali al passo con le minacce informatiche di oggi.

Gestione delle politiche di tutela della privacy

- Progettato in conformità alle raccomandazioni ISO 37002:2021 e Direttiva UE 2019/1937 per la conformità al whistleblowing.
- Supporta la comunicazione anonima bidirezionale (commenti/messaggi).
- Flusso di lavoro di gestione dei casi personalizzabile (stati/sottostati).
- Flusso di lavoro di segnalazione condizionale basato sull'identità del whistleblower.
- Gestisce i conflitti di interesse nel flusso di lavoro di segnalazione.
- Funzionalità di custodia per autorizzare l'accesso all'identità del whistleblower.
- Privacy GDPR by design e by default.
- Policy di conservazione dei dati GDPR configurabili.
- Modulo di sottoscrizione conforme al GDPR per nuovi utenti SaaS.
- Nessuna registrazione degli indirizzi IP.
- Include un registro di controllo.
- Software libero Licenza AGPL 3.0 approvata da OSI.

Gestione dei rischi

L'analisi dei rischi viene condotta secondo metodologia CNIL (o altra metodologia definita dal Titolare).

Accesso illegittimo ai dati

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

Diffusione indesiderata dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Mobbing, Discriminazioni lavorative, Ritorsioni

Quali sono le principali minacce che potrebbero concretizzare il rischio?

furto dati accesso account operatore, diffusione voluta o indesiderata della segnalazione a terzi

Quali sono le fonti di rischio?

collaboratori, operatori, dipendenti, collaboratori di fornitori ente

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

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

Limitata: I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative, Ritorsioni.

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

Trascurabile: Le misure di sicurezza hardware e software adottate rendono trascurabile la probabilità del rischio. La gestione limitata del numero di operatori abilitati alla gestione delle segnalazione rende, parimenti, trascurabile tale rischio.

Modifiche indesiderate dei dati

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

Consultazione dei propri da parte di personale non autorizzato, Discriminazioni lavorative, Mobbing, Ricatto economico, Ritorsioni, Diffusione indesiderata dati

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

diffusione voluta o indesiderata della segnalazione a terzi, furto dati accesso account operatore

Quali sono le fonti di rischio?

collaboratori, dipendenti, operatori, collaboratori di fornitori ente

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

Controllo degli accessi logici, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione dei rischi

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

Limitata: I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.

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

Trascurabile: Le misure di sicurezza hardware e software adottate rendono trascurabile la probabilità del rischio. La gestione limitata del numero di operatori abilitati alla gestioned delle segnalazione rende, parimenti, trascurabile tale rischio.

Perdita di dati

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

Consultazione dei propri da parte di personale non autorizzato, Diffusione indesiderata dati, Mobbing, Ricatto economico, Discriminazioni lavorative, Ritorsioni

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

diffusione voluta o indesiderata della segnalazione a terzi, furto dati accesso account operatore

Quali sono le fonti di rischio?

collaboratori, dipendenti, collaboratori di fornitori ente, operatori

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

Crittografia e Sicurezza Canali Informatici, Controllo degli accessi logici, Tracciabilità, Archiviazione, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione delle politiche di tutela della privacy, Gestione dei rischi

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

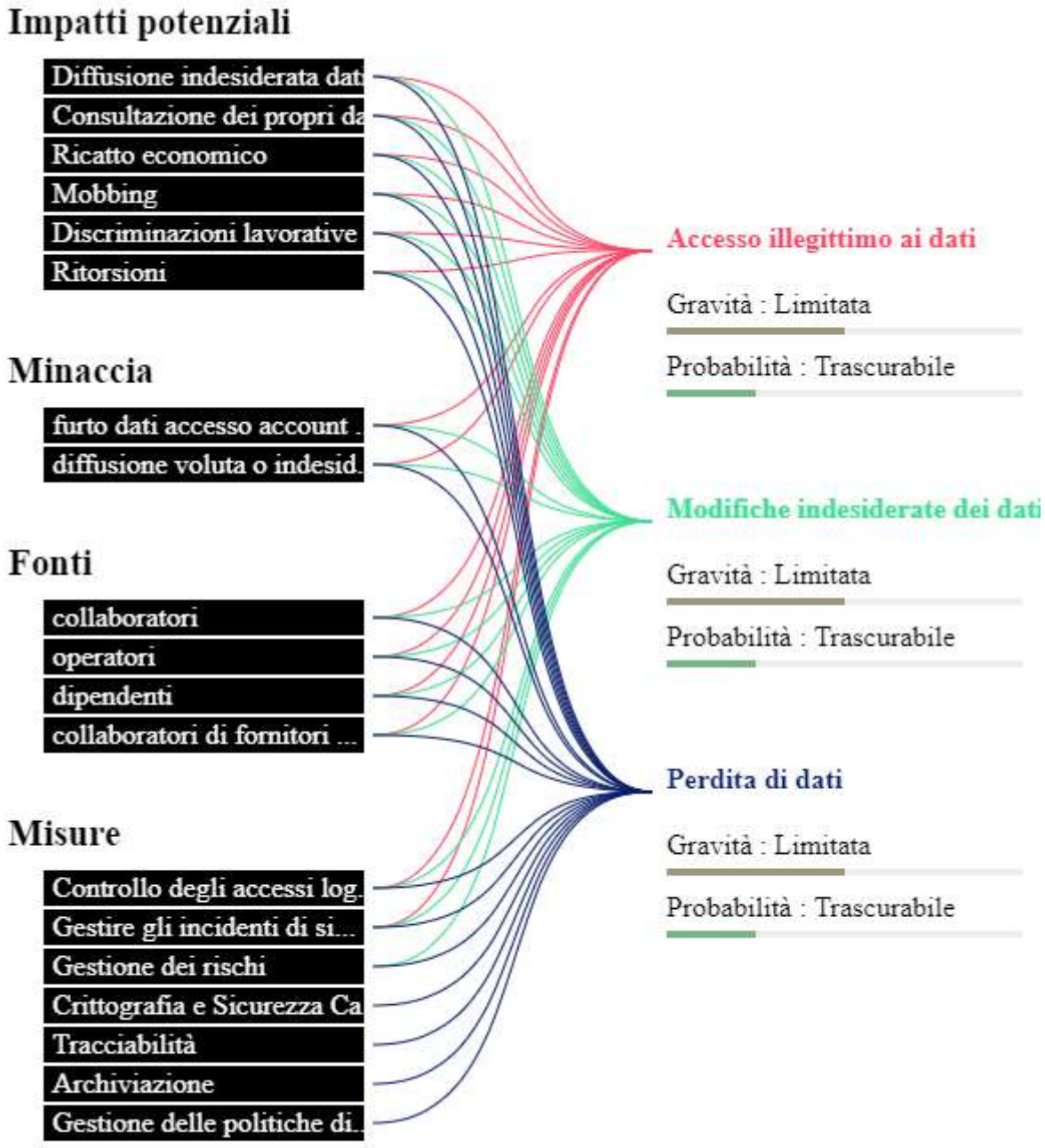
Limitata: I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.

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

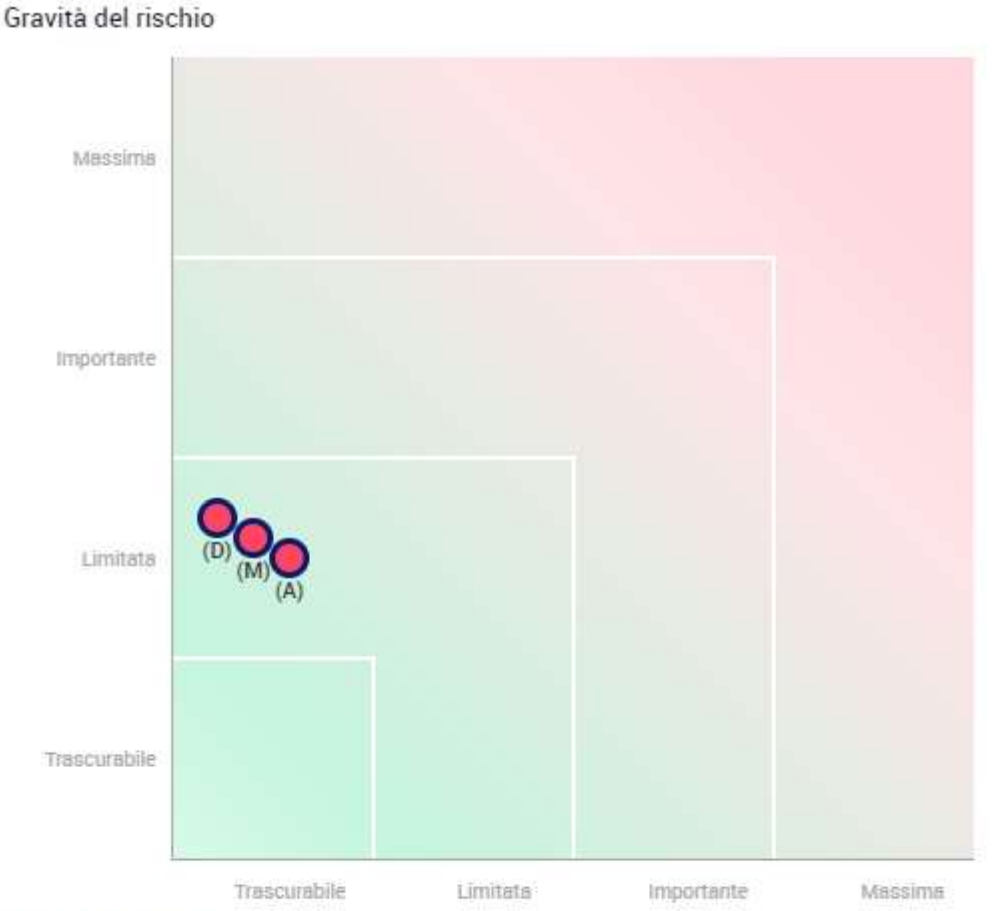
Trascurabile: Le misure di sicurezza hardware e software adottate rendono trascurabile la probabilità del rischio. La gestione limitata del numero di operatori abilitati alla gestione delle segnalazione rende, parimenti, trascurabile tale rischio.

Panoramica dei rischi

Mappaggio dei rischi



Gravità del rischio



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

4. Validazione

Opinione del DPO/RPD:

Nome del DPO/RPD

Ing. Giombattista Migliore

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

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.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

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.