DPIA

Informazioni sulla PIA

Nome della PIA: SEGNALAZIONI DI VIOLAZIONI DELLE DISPOSIZIONI NORMATIVE AI SENSI DEL DECRETO LEGISLATIVO 10 MARZO 2023, n. 24 (WHISTLEBLOWING) (forma scritta/orale)

Nome autore	Data di creazione	Nome del DPO/RPD
Dott. Roberto Calvani	12 ottobre 2023	Paolo Vicenzotto

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si ritiene opportuno procedere alla richiesta di alcun parere agli Interessati.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento oggetto di valutazione con la presente DPIA riguarda la gestione della raccolta delle segnalazioni whistleblowing attraverso il seguente canale di segnalazione interno: segnalazione effettuata tramite **forma scritta**, a mezzo del servizio postale o tramite posta interna in una busta chiusa che rechi all'esterno la dicitura "riservata/personale", o in **forma orale**, attraverso la linea telefonica diretta del RPCT ovvero, su richiesta, mediante un incontro diretto con il RPCT.

Quali sono le responsabilità connesse al trattamento?

Le segnalazioni vengono trattate esclusivamente dal RPCT

Ci sono standard applicabili al trattamento?

Attualmente non esistenti per il trattamento oggetto della presente valutazione.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati personali raccolti e trattati nell'ambito della segnalazione possono includere dati personali "comuni" del "Segnalante", del "Segnalato" e delle persone coinvolte e/o collegate ai fatti oggetto della segnalazione (ad es. dati anagrafici, funzioni, recapiti quali: indirizzo mail, indirizzo postale, numero telefonico, dati sulla qualifica professionale ricoperta, dati e informazioni ulteriori connessi alla condotta illecita. E' possibile che, in alcuni casi, ove necessario, siano altresì trattati appartenenti a particolari categorie ex art. 9 e/o 10 del GDPR.

Qual è il ciclo di vita del trattamento dei dati?

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

Quali sono le risorse di supporto ai dati?

La segnalazione potrà essere effettuata tramite forma scritta, a mezzo del servizio postale o tramite posta interna in una busta chiusa che rechi all'esterno la dicitura "riservata/personale", o in forma orale, attraverso la linea telefonica diretta del RPCT ovvero, su richiesta, mediante un incontro diretto con il RPCT. Per la segnalazione si utilizza una linea telefonica non registrata e la segnalazione è documentata per iscritto mediante resoconto dettagliato della conversazione a cura del RPCT. La persona segnalante può verificare, rettificare e confermare il contenuto della trascrizione mediante la propria sottoscrizione.
Quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il RPCT, essa, previo consenso della persona segnalante, è documentata a cura del RPCT mediante verbale.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Lo scopo del trattamento è permettere di segnalare condotte illecite all'interno dell'Ente. Si precisa che, per poter godere delle tutele previste dal D. Lgs. 24/23, gli illeciti devono essere conosciuti in virtù del rapporto di lavoro ovvero in occasione dello svolgimento del rapporto di servizio o fornitura o realizzazione di opera in favore dell'Ente.

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento è lecito ai sensi dell'art. 6 par. 1 lett. C ed E del GDPR. Alcuni trattamenti specifici, si basano inoltre sul consenso del segnalante.

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

Il segnalante è tenuto a fornire tutti gli elementi utili a consentire agli uffici competenti di procedere alle dovute e appropriate verifiche a riscontro della fondatezza dei fatti oggetto di segnalazione. A tal fine, la segnalazione deve preferibilmente contenere i seguenti elementi:
a) generalità del soggetto che effettua la segnalazione con indicazione della posizione o funzione svolta nell'ambito dell'Ente;
b) la chiara e completa descrizione dei fatti oggetto di segnalazione;
c) se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi;
d) se conosciute, le generalità o altri elementi (come la qualifica e il servizio in cui svolge l'attività) che consentano di identificare il soggetto che ha posto in essere i fatti oggetto di segnalazione;
e) l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
f) l'indicazione di eventuali documenti che possono confermare la fondatezza di tali fatti;
g) ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

I dati sono esatti e aggiornati?

Non applicabile al trattamento in oggetto.

Qual è il periodo di conservazione dei dati?

Il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati attraverso l'informativa privacy specifica messa a disposizione in fase di presentazione della segnalazione ed attraverso la procedura per poter effettuare la segnalazione. Entrambi i documenti sono pubblicati all'interno del sito web istituzionale.

Gli interessati sono messi in grado di esercitare i diritti di cui agli artt. 15 e seguenti?

Si, con le modalità indicate nell'informativa del punto precedente.

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

Non applicabile al trattamento in oggetto.

I dati sono trasferiti al di fuori del territorio UE?

No.

Rischi

Indisponibilità dei dati (distruzione, perdita, furto)

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

Possibili ritorsioni sul segnalante e altre persone coinvolte (es. colleghi di lavoro); impatti psicologici per diffusione del nominativo del segnalante; impatti sui diritti alla libertà del segnalante (es. telefonate, e- mail o altro di comunicazioni indesiderate)

Quali sono le principali minacce che potrebbero concretizzare il rischio?

attacchi fisici: azioni offensive finalizzate a distruggere, esporre, alterare, disabilitare, sottrarre o ottenere l'accesso non autorizzato a risorse fisiche come i locali fisici e le attrezzature. Si tratta generalmente di atti di vandalismo, furto, sabotaggio, perdita di informazioni e attacchi massivi. Questo tipo di minaccia può ovviamente riguardare qualsiasi tipo di infrastruttura

Quali sono le fonti di rischio?

Personale interno all'organizzazione, persone esterne, eventi naturali e non naturali

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Protezione dei locali fisici, protezione della documentazione

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

L'impatto sugli interessati avrebbe un livello ALTO, visti gli impatti potenziali a danno del segnalante e delle altre persone coinvolte

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

Improbabile per la distruzione; probabile per quanto riguarda le minacce di perdita e furto della documentazione

Integrità dei dati (alterazione, modifica)

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

Possibili ritorsioni sul segnalante e altre persone coinvolte (es. colleghi di lavoro); impatti psicologici; impatti sui diritti alla libertà del segnalante (es. telefonate, e- mail o altro di comunicazioni indesiderate)

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

attacchi fisici: azioni offensive finalizzate a distruggere, esporre, alterare, disabilitare, sottrarre o ottenere l'accesso non autorizzato a risorse fisiche come i locali fisici e le attrezzature. Si tratta generalmente di atti di vandalismo, furto, sabotaggio, perdita di informazioni e attacchi massivi. Questo tipo di minaccia può ovviamente riguardare qualsiasi tipo di infrastruttura

Quali sono le fonti di rischio?

Personale interno all'organizzazione, persone esterne

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

Protezione dei locali fisici, protezione della documentazione

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

L'impatto sugli interessati avrebbe un livello ALTO, visti gli impatti potenziali a danno del segnalante e delle altre persone coinvolte

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

Improbabile: c'è una bassa possibilità che i fascicoli cartacei subiscano delle alterazioni

Riservatezza dei dati (accesso abusivo, trattamento non conforme)

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

Possibili ritorsioni sul segnalante e altre persone coinvolte (es. colleghi di lavoro); impatti psicologici per diffusione del nominativo del segnalante; impatti sui diritti alla libertà del segnalante (es. telefonate, e- mail o altro di comunicazioni indesiderate)

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

attacchi fisici: azioni offensive finalizzate a distruggere, esporre, alterare, disabilitare, sottrarre o ottenere l'accesso non autorizzato a risorse fisiche come i locali fisici e le attrezzature. Si tratta generalmente di atti di vandalismo, furto, sabotaggio, perdita di informazioni e attacchi massivi. Questo tipo di minaccia può ovviamente riguardare qualsiasi tipo di infrastruttura

Quali sono le fonti di rischio?

Personale interno all'organizzazione, persone esterne

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

Protezione dei locali fisici, protezione della documentazione

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

L'impatto sugli interessati avrebbe un livello ALTO, visti gli impatti potenziali a danno del segnalante e delle altre persone coinvolte

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

Probabile: c'è una ragionevole possibilità che le minacce si materializzino

Piano d'azione

Misure e Procedure adottate o programmate per la mitigazione dei rischi

Individuazione di strumenti di protezione dei locali e degli armadi contenenti la documentazione cartacea

Parere del DPO/RPD:

L'autore dott. Roberto Calvani

Il Validatore / DPO avv. Paolo Vicenzotto