INFORMAZIONI SULLA DPIA

(valutazione dell'impatto connesso all'uso di tecnologie digitali)

Nome della Pia
Servizio Piattaforma Whistleblowing

Nome validatore
Carmine Arricale

Premessa

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**,** 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 valutazione d'impatto (DPIA), si effettua sulla valutazione del rischio preso in considerazione dal servizio offerto dalla Piattaforma GlobaLeafis, di cui Whistleblowing Solutions è co-autore e coordinatore, utilizzata dal Comune di Duronia., in relazione al passaggio di dati che avviene per tale servizio per la protezione dei dati.

Normativa di riferimento

Ai fini della redazione del presente atto di fa riferimento specificatamente ai seguenti atti normativi:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato e integrato dal Decreto Legislativo 10 agosto 2018 n.101;
- Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) [Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679 Versione adottata l'11 aprile 2018];

- Decreto Legislativo 18 agosto 2000, n. 267. Testo unico delle leggi sull'ordinamento degli enti locali.
- Legge 30 Novembre 2017, n. 179 “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.”
- Legge 6 Novembre 2012, n. 190 “Disposizioni per la prevenzione e la repressione della corruzione e della illegalità nella pubblica amministrazione.”
- Decreto Legislativo 10 marzo 2023, n. 24 “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.”

Valutazione del Contesto

Dati del DPO: avv. Carmine Arricale -
mail: dott.carmine.arricale@gmail.com - PEC: avv.carminearricale@legalmail.it

Parere del DPO/RPD:
Allo stato attuale dei sistemi tecnologici e con le informazioni attualmente disponibili per l’organizzazione interessata il trattamento si ritiene accettabile e implementabile.

Motivazione della mancata richiesta del parere degli interessati
Il fondamento giuridico del trattamento dei dati risiede nell'assolvimento di funzioni ed obblighi di legge

Panoramica del trattamento

Quale è il trattamento in considerazione?

La **piattaforma GlobaLeafis** di cui Whistleblowing Solutions è co-autore e coordinatore utilizzata dal Comune di Duronia. Essa svolge funzioni di raccolta e gestione delle segnalazioni di illeciti per contrastare fenomeni corruttivi, sia nelle imprese private sia nellepubbliche amministrazioni.

Quali sono le responsabilità connesse al trattamento in questione?

Titolare del trattamento dei dati personali è il Comune di Duronia.
Responsabile o Incaricato del trattamento dei dati, secondo le scelte del titolare del trattamento dei dati, è il responsabile p.t. della prevenzione della corruzione.

Ci sono standard applicabili al trattamento?

Utilizzo di politiche privacy indicate nel Registro del Trattamento, in particolare si applicheranno le linee guida del EDPB e del Garante nazionale per la protezione dei dati.

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

La piattaforma informatica utilizzata consente la compilazione, l’invio e la ricezione delle

segnalazioni di presunti fatti illeciti nonché la possibilità per l'ufficio del Responsabile della prevenzione corruzione (RPC), che riceve tali segnalazioni, di comunicare in forma riservata con il segnalante senza conoscerne l'identità.

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

Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonché dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33. Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del decreto legislativo 24 del 2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

Quali sono le risorse di supporto ai dati?

I dati sono gestiti mediante un'apposita piattaforma dal Comune di Duronia basata sul riuso del software GlobaLeafis, per l'acquisizione e la gestione - nel rispetto delle garanzie di riservatezza previste dalla normativa vigente - delle segnalazioni di illeciti da parte dei dipendenti dell'Ente, dialogare con i segnalanti anche in modo anonimo così come previsto dal Decreto Legislativo 24 del 2023 e previstodalle Linee Guida Anac. GlobaLeafis è un software open-source creato per permettere l'avvio di iniziative di whistleblowing sicuro ed anonimo rilasciato sotto licenza.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento in questione comporta il conferimento al Responsabile della Prevenzione della Corruzione (RPC) dell'ente, tramite compilazione di un form su apposita procedura web, di dati anagrafici, codice fiscale, dati di contatto e, eventualmente, dati sulla qualifica professionale, nonché di dati e informazioni ulteriori connessi alla condotta illecita riportata.
I dati forniti verranno trattati esclusivamente per l'istruttoria della segnalazione ai sensi del Decreto Legislativo 24 del 10 marzo 2023.
Al fine di garantire la riservatezza del segnalante per tutta la durata della gestione della segnalazione, l'identità dello stesso sarà conosciuta solo dal Responsabile della Prevenzione della Corruzione (RPC) dell'ente. Ad eccezione dei casi in cui sia configurabile una responsabilità a titolodi calunnia e di diffamazione ai sensi delle disposizioni del codice penale o dell'art. 2043 del codicecivile e delle ipotesi in cui l'anonimato non sia opponibile per legge (ad esempio, indagini penali, tributarie o amministrative, ispezioni di organi di controllo), l'identità del segnalante viene protetta in ogni contesto successivo alla segnalazione. Pertanto, fatte salve le citate eccezioni, l'identità del segnalante non può essere rivelata senza il suo espresso consenso, e tutti coloro che ricevono o sonocoinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza di tale informazione.

In questo ambito, i trattamenti di dati personali effettuati dai soggetti obbligati possono essere considerati necessari per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, § 1, lett. c) del Regolamento), e, con riguardo a categorie particolari di dati (art. 9, § 2, lett. b) del Regolamento in relazione all'art. 54-bis,) o a dati relativi a condanne penali e reati, possono, altresì, essere considerati necessari per l'esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (art. 6, § 1, lett. e) e art. 9, § 2, lett. g) e 10 del Regolamento). Il trattamento dei dati personali è improntato ai principi di correttezza, liceità e trasparenza e di tutela della riservatezza e dei diritti dell'interessato, nonché agli ulteriori principi previsti dall'art. 5 del Regolamento.
Tali attività sono esplicitate attraverso specifica informativa ai sensi dell'articolo 13 del Regolamento Ue 679/2016.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento si basa sulle competenze attribuite dalla legge all'ente e, tra le altre, in particolare dal d.lgs.267/2000 "Testo Unico degli Enti Locali", dalla Legge 30 Novembre 2017, n. 179 "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.", dalla Legge 6 Novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e della illegalità nella pubblica amministrazione.", dal Decreto Legislativo 10 marzo 2023, n. 24 "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali."

Valutazione: Accettabile

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

In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'articolo 5 , paragrafo 1, lettera c) RGPD, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione dei dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
Il trattamento dei dati personali verrà effettuato esclusivamente dal Responsabile della Prevenzione della Corruzione (RPC) dell'ente, con l'utilizzo di procedure anche informatizzate, dotate di strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e del contenuto delle segnalazioni e della relativa documentazione, adottando misure tecniche e organizzative adeguate a proteggerli da accessi non autorizzati o illeciti, dalla distruzione, dalla perdita d'integrità e riservatezza, anche accidentali.
I dati verranno conservati per 5 anni e comunque per tutta la durata dell'eventuale procedimento disciplinare, penale o dinanzi la Corte dei Conti.I dati personali non saranno comunicati ad altri soggetti, ad esclusione dei casi sopra indicati, così come non saranno oggetto di diffusione.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

Al fine della verifica della correttezza e dell'aggiornamento dei dati si stabilisce la prima verifica entro un anno dalla redazione del presente documento.
Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Ai sensi dell'articolo 14 del D. Lgs. 24 del 10 marzo 2023 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 a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del decreto legislativo citato e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Ai sensi dell'articolo 13 del D. Lgs. 24 del 10 marzo 2023, ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti viene effettuato a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51.
I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente. Sono fornite idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato decreto legislativo n. 51 del 2018.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso degli interessati non è richiesto in quanto il fondamento giuridico del trattamento risiede nell'assolvimento di funzioni ed obblighi di legge.

Valutazione: Accettabile

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

Gli interessati del trattamento hanno diritto di ottenere dall'ente, nei casi previsti dal Regolamento, l'accesso ai dati personali, la rettifica, l'integrazione, la cancellazione degli stessi o la limitazione del trattamento ovvero di opporsi al trattamento medesimo (artt. 15 e ss. del Regolamento).

L’interessato potrà esercitare tutti i diritti di cui sopra inviando una e-mail al Responsabile della prevenzione della corruzione (RPC) all’indirizzo di posta elettronica personale disponibile alla home page dell’ente o inviando una pec all' indirizzo: duroniacomune@postecert.it.
Gli interessati che ritengano che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dal Regolamento hanno, inoltre, il diritto di proporre reclamo all’Autorità Garante per la protezione dei dati personali, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).
Nella informativa presente sulla home page istituzionale dell’Ente è indicato il riferimento del titolare del trattamento, del DPO/RDP e del Garante Italiano per la protezione dei dati personali, con gli indirizzi mail e fisici, ai quali rivolgersi per avere informazioni ovvero per segnalare eventuali violazioni.

Valutazione: Accettabile

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.

Valutazione: Accettabile

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

L’interessato potrà esercitare i diritti di limitazione ed opposizione inviando una e-mail al Responsabile della prevenzione della corruzione (RPC) all’indirizzo di posta elettronica personale disponibile alla home page dell’ente o inviando una pec all' indirizzo: duroniacomune@postecert.it.
Nella informativa presente sulla home page istituzionale dell’Ente è indicato il riferimento del titolare del trattamento, del DPO/RDP, del RCP, del Garante Italiano per la protezione dei dati personali, con gli indirizzi mail e fisici, ai quali rivolgersi per avere informazioni ovvero per segnalare eventuali violazioni.

Valutazione: Accettabile

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

Sono contenute nell'atto di designazione a responsabile del trattamento e in quello di nomina a responsabile della prevenzione della corruzione. Il contratto non è previsto in quanto egli è già legato da un rapporto contrattuale con l'Ente e pertanto la nomina e le indicazioni derivano da atto autoritativo di diritto amministrativo.

Valutazione: Accettabile

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

Non è previsto alcun trasferimento al di fuori dell'Unione Europea.

Valutazione: Accettabile

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

Non è previsto alcun trasferimento al di fuori dell'Unione Europea.

Valutazione: Accettabile

Valutazione del sistema

Misure esistenti o pianificate

Crittografia

I dati sono gestiti mediante un'apposita piattaforma attivata dal Comune di Duronia basata sul riuso del software GlobaLeafis, per l'acquisizione e la gestione - nel rispetto delle garanzie di riservatezza previste dalla normativa vigente - delle segnalazioni di illeciti da parte dei dipendenti dell'Ente, dialogare con i segnalanti anche in modo anonimo così come previsto dal Decreto Legislativo 24 del 2023 e previstodalle Linee Guida Anac. GlobaLeafis è un software open-source creato per permettere l'avvio di iniziative di whistleblowing sicuro ed anonimo certificato.
L'applicazione utilizza un protocollo di crittografia che garantisce la protezione dei dati identificativi dell'identità del segnalante, mentre il codice identificativo univoco ottenuto a seguito della segnalazione registrata sul portale consente al segnalante di "dialogare" in modo anonimo e spersonalizzato.

Valutazione: Accettabile

Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati dal responsabile per la prevenzione della corruzione e della trasparenza che verifica che siano disposti in specifici raccoglitori in modo tale che non vadano dispersi e che non siano visibili a terzi non autorizzati, gli uffici devono essere chiusi e l'accesso consentito soltanto agli addetti o i soggetti autorizzati.

Valutazione: Accettabile

Specifiche Misure di Sicurezza

Il Titolare del trattamento e il responsabile per la prevenzione della corruzione, previa valutazione dei rischi, mettono in atto misure volte a:

- vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);
- impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);
- impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);
- impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);
- garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);
- garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);
- garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);
- impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);
- garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);
- garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Valutazione: Accettabile

Accesso illegittimo ai dati

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

Qualora fosse realizzato un accesso abusivo al sistema da soggetti attrezzati e travisati e fosse possibile asportare la memoria di massa senza il pronto intervento dei sistemi di sicurezza, i dati sarebbero crittografati, Quindi si tratterebbe di un impatto limitato

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Furto, Accesso illegittimo

Quali sono le fonti di rischio?

interne, esterne, non umane

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Specifiche Misure di Sicurezza

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

Limitato, poiché il sistema di crittografia e il posizionamento del computer di accesso in un locale sicuro e presidiato qual è l'ufficio del responsabile per la prevenzione della corruzione e della trasparenza rendono molto limitato il rischio di accesso abusivo ai dati e limitato il rischio di distruzione degli stessi.

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

Limitata, sulla base delle misure pianificate.

Valutazione: Accettabile

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)? Limitata

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)? Limitata

Modifiche indesiderate dei dati

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

Qualora fosse realizzato un accesso abusivo al sistema da soggetti attrezzati e travisati e fosse possibile asportare la memoria di massa senza il pronto intervento dei sistemi di sicurezza, i dati sarebbero crittografati, Quindi si tratterebbe di un impatto limitato

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

Errore materiale, evento doloso o abuso/violazione da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

Quali sono le fonti di rischio?

esterne, interne, non umane

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

Specifiche Misure di Sicurezza, Sicurezza dei documenti cartacei

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

Limitata, il sistema di crittografia e il controllo logico degli accessi rende pressoché impossibile l'accesso ai dati ai fini della modifica se non ai soggetti autorizzati e quindi formati e competenti.

Valutazione: Accettabile

Perdita di dati

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

Perdita delle informazioni

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

Errore materiale, Furto, Vandalismo, danno o malfunzionamento del sistema di registrazione dei dati.

Quali sono le fonti di rischio?

esterne, interne, non umane

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

Specifiche Misure di Sicurezza, Sicurezza dei documenti cartacei

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

Limitata, in quanto il server che ospita il servizio è collocato in ambiente cloud in grado di garantire un elevato livello di resilienza ai guasti e ai disservizi nonché da un giornaliero backup delle informazioni fatto da una società esterna a cui è affidato il servizio

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

Limitata, i sistemi di sicurezza adottati rendono trascurabile il rischio.

Mappa dei rischi

Gravità: trascurabile

Piano d'azione

A valle dell'indagine della DPIA condotta l'attività ricade in fascia BASSA.

DPO
Avv. Carmine Arricale

CARMINE ARRICALE
30.11.2023
12:41:45 UTC