COMUNE DI TURI

(Città Metropolitana di Bari)

DPIA (DATA PROTECTION IMPACT ASSESSMENT)
VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI
PIATTAFORMA WHISTLEBLOWING

(art. 35 Regolamento UE/2016/679 GDPR)

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."*

DPIA (DATA PROTECTION IMPACT ASSESSMENT)
VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI
PIATTAFORMA WHISTLEBLOWING

Normativa di Riferimento

Ai fini della redazione del presente atto si 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."*

Soggetto Designato al trattamento dei Dati: COMUNE DI TURI
DPO Comune di TURI: Rete Entionline all privacy

Parere DPO: in base alla documentazione fornita da Digital.PA la Piattaforma Whistleblowing è stata ritenuta adeguata ai fini della predisposizione del DPIA.

Mappatura dei rischi

Piano d'azione

Principi fondamentali

CONTESTO

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il Comune di Turi ha acquisito il servizio per la gestione delle segnalazioni di illecito tramite piattaforma digitale Whistleblowing. Il soggetto Responsabile del Trattamento dei dati è la società Digital P.A. S.r.l. che si occupa della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.
ARCHITETTURA DI SISTEMA
Il servizio viene erogato in S.a.a.S. (Software as a Service), garantendo la terzietà del sistema.
Sono garantiti continui aggiornamenti di sicurezza del software ed efficienza dell'Help Desk dedicato. È, quindi, un software accessibile tramite la rete internet esclusivamente attraverso il protocollo HTTPS ed è ottimizzato per la visualizzazione su qualsiasi recente browser.
I dati inseriti nel sistema vengono cifrati sia nella trasmissione, tramite il protocollo HTTPS, sia in memorizzazione, tramite un avanzato sistema di cifratura.
Il processo di Registrazione è separato dalla segnalazione, il che consente la gestione delle segnalazioni riservate (nelle quali il segnalante è identificabile) in maniera anonima.
La piattaforma web Segnalazione Illeciti - Whistleblowing si suddivide in un Portale pubblico / Ambiente di Segnalazione dedicato ai segnalanti e un Pannello gestionale / Area di Amministrazione dedicato al Responsabile della segnalazione (o ai Responsabili e ad eventuali Collaboratori incaricati).
I segnalanti possono inviare la segnalazione anche attraverso l'App Legality Whistleblowing, collegata alla piattaforma web.

SOFTWARE IMPIEGATO

La piattaforma informatica di segnalazione è basata sul software **Legality Whistleblowing** di proprietà di Digital P.A. s.r.l..

Sono garantiti continui aggiornamenti di sicurezza del software ed efficienza dell'Help Desk dedicato. È, quindi, un software accessibile tramite la rete internet esclusivamente attraverso il protocollo HTTPS ed è ottimizzato per la visualizzazione su qualsiasi recente browser.

Architettura di Rete

● Il sistema è installato su una infrastruttura di Server Dedicati certificata TIER IV, che garantisce le migliori prestazioni in termini di sicurezza e di disponibilità dei dati.

Quali sono le responsabilità connesse al trattamento?

Titolare della piattaforma: Comune di TURI

Designato: il titolare procede, con decreto sindacale, a nominare quale soggetto "designato" al trattamento dei dati personali il Responsabile della Prevenzione della Corruzione e in sostituzione il Responsabile del Settore AA.II. Nell'atto di designazione sono indicati i compiti ed i poteri del designato. Il soggetto designato al coordinamento delle attività e al controllo procede al trattamento dei dati attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari. Procede all'individuazione ed alla nomina dei soggetti autorizzati e dei soggetti responsabili del trattamento ai sensi dell'art.28 GDPR.

Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing: DigitalPA S.r.l.

Soggetti autorizzati: Il funzionario designato al coordinamento delle attività e al controllo del trattamento dei dati procede ad individuare con proprio atto le persone fisiche autorizzate al trattamento dei dati, all'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, alla visione delle registrazioni nonché all'acquisizione delle stesse. L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato anche attraverso una nomina legata alla funzione.

Ci sono standard applicabili al trattamento?

- ISO27001
- ISO22301:2019
- Qualifica AGID

Valutazione : Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti.

Dati di registrazione

Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione).

Categorie particolari di dati

Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.

Dati relativi a condanne penali e reati

Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

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

1. Attivazione della piattaforma
2. Configurazione della piattaforma
3. Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti
4. Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore.

Principi Fondamentali

Finalità del trattamento

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati vengono trattati per dare applicazione all'Istituto del Whistleblowing disciplinato dall'art. 54 bis del D.lgs 165/2001, secondo le indicazioni contenute nelle «Linee guida in materia di tutela del dipendente pubblico che segnala illeciti" di cui alla Delibera ANAC n. 469 del 9 giugno 2021". La finalità del trattamento, pertanto è lecita in quanto eseguita per le finalità indicate da norma di Legge.
Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

- Art. 54 bis del d.lgs. n. 165/2001 così come modificato dalla legge 30 novembre 2017, n. 179;
- Delibera ANAC n. 469 del 9 giugno 2021 «Linee guida in materia di tutela del dipendente pubblico che segnala illeciti"

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)?

I dati richiesti per la segnalazione sono quelli indispensabili per il contatto del segnalante, sempre che questi non decida per l'anonimato. Tutte le informazioni che possono rivelare i contenuti di una segnalazione e l'identità del suo autore, o che possono dare indicazioni sull'attività di un segnalante, sono comunque protette da un sistema di cifratura.
Le segnalazioni (comprese le bozze), gli allegati (anche quelli temporanei), i log di attività e le sessioni sono cifrate.
Inoltre, non esiste alcuna correlazione diretta tra utente della piattaforma (segnalante) ed eventuali segnalazioni
Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata.
Valutazione : Accettabile

I dati sono esatti e aggiornati?

L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata.
Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.
Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

Policy di data retention di default delle segnalazioni di 18 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute.
Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.
Valutazione: accettabile.

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

INFORMAZIONI NECESSARIE
Gli interessati vengono informati delle finalità del trattamento dei dati, dei tempi di conservazione e delle modalità di trattamento con informativa specifica sul trattamento dei dati ai sensi dell'art. 13 del Reg. UE 2016/679.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

NA
Valutazione : Accettabile

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

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., GDPR, su presentazione di apposita istanza, ha diritto:
a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 GDPR, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, GDPR.
2. L'istanza per l'esercizio dei diritti dell'interessato è presentata al soggetto designato il quale, eventualmente previa consultazione con il DPO (Responsabile della Protezione dei dati) dell'Ente decide in merito.
3. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.
Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.
Valutazione : Accettabile

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

Il soggetto interessato ha diritto di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 GDPR, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati.
1. L'istanza per l'esercizio dei diritti dell'interessato è presentata al soggetto designato il quale, eventualmente previa consultazione con il DPO (Responsabile della Protezione dei dati) dell'Ente decide in merito.
Valutazione : Accettabile

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

1. Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, GDPR ed alle previsioni Decreto Legislativo 101/2018 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, 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", in attuazione della delega al Governo di cui all'art. 13, L. 163/2017.

Valutazione : Accettabile

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

Gli accordi contrattuali sono definiti con le seguenti società:

- Digital PA s.r.l. in qualità di Responsabile del trattamento

Valutazione : Accettabile

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

I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea.
Non esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

Sulla piattaforma Segnalazione Illeciti - Whistleblowing tutte le informazioni che possono rivelare i contenuti di una segnalazione e l'identità del suo autore, o che possono dare indicazioni sull'attività di un segnalante, sono protette da un sistema di cifratura.

Le segnalazioni (comprese le bozze), gli allegati (anche quelli temporanei), i log di attività e le sessioni sono cifrate.

Inoltre, non esiste alcuna correlazione diretta tra utente della piattaforma (segnalante) ed eventuali segnalazioni.

I messaggi scambiati in quest'area sono protetti con crittografia asimmetrica e sono decifrabili esclusivamente dal destinatario del messaggio tramite la specifica piattaforma software.

Valutazione : Accettabile

Controllo degli accessi logici

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.

Gli accessi ai server sono registrati come da regolamento UE, e in base alla normativa Italiana, su dispositivo Write-Once Read-Many (WORM) e criptati. I log in questo modo possono essere analizzati per le verifiche programmate. Periodo di conservazione predefinito: 181 giorni.

L'accesso ai log è consentito esclusivamente al Responsabile delle Segnalazioni. Per ogni voce di log memorizzata viene generata una chiave simmetrica KsimL. La KsimL viene cifrata sia con la KpubR che con la chiave pubblica degli Amministratori del sistema KpubA.

La decifratura avviene utilizzando le rispettive chiavi private decodificate attraverso la password usata all'atto del login

Valutazione : Accettabile

Tracciabilità

Tutte le operazioni effettuate sulle segnalazioni, da parte di tutti gli utenti, vengono registrate nei Log di sistema in maniera anonima e criptata per garantire la massima riservatezza e anonimato.

I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.

I log degli accessi degli amministratori di sistema vengono registrati tramite registri remoti centralizzati.

Valutazione : Accettabile

Archiviazione

Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.
Valutazione : Accettabile

Gestione delle vulnerabilità tecniche

L'applicativo e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review.

Valutazione : Accettabile

Backup

I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.

Valutazione : Accettabile

Manutenzione

E' prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza.

Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Digital PA s.r.l. attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Valutazione : Accettabile

Sicurezza dei canali informatici

Tutte le connessioni sono protette tramite protocollo TLS 1.2.

Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.

Valutazione : Accettabile

Sicurezza dell'hardware

I datacenter sono protetti da:
• *Doppio portoncino blindato*
• *Antifurto a sensore di apertura porte e sensore volumetrico/infrarosso a doppia tecnologia e dispositivo di alert sms ed email e app mobile.*
• *Videosorveglianza full hd interna ed esterna ai locali 24h*365 con riversamento su NAS dedicato*
• *L'accesso ai locali è profilato attraverso le chiavi antifurto personale in dotazione ai soli responsabili con diverse abilitazioni e fasce orarie di accesso.*
• *L'accesso ai locali durante gli orari lavorativi è consentito tramite inserimento di codice da digitare su tastiera posta all'ingresso*
• *È vietato l'accesso non autorizzato al di fuori degli orari lavorativi. Gli accessi ai responsabili muniti di chiavi di accesso vengono monitorati dai log di accesso ai locali tramite chiave personalizzata dell'antifurto.*
• *Presenza di estintori a polvere revisionati*
Per ulteriori dettagli, consultare il documento "Modelli di erogazione in SaaS"
I datacenter sono certificati ISO27001.
Valutazione : Accettabile

Vigilanza sulla protezione dei dati

Titolare, soggetto designato e DPO verificano la correttezza del trattamento.

Valutazione : Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Digital PA s.r.l. ha definito una procedura per la gestione delle violazioni dei dati personali.

Valutazione : Accettabile

Lotta contro il Malware

Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware.

Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

Valutazione : Accettabile

RISCHI

<u>Accesso illegittimo ai dati</u>

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

Perdita di riservatezza, azioni ritorsive.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso abusivo, perdita di confidenzialità

Quali sono le fonti di rischio?

Personale operante, Soggetti terzi

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Tracciabilità, Controllo degli accessi logici, Politica di tutela della privacy, Gestione delle vulnerabilità tecniche, Anonimizzazione, Crittografia

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

Importante, la riservatezza dei dati dei soggetti che effettuano segnalazioni è elemento determinante del whistleblowing.

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

Trascurabile, e' improbabile che il personale proceda alla divulgazione delle segnalazioni o che vi sia un accesso abusivo al database
Valutazione : Accettabile

RISCHI

<u>Modifiche indesiderate dei dati</u>

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

Perdita di riservatezza, azioni ritorsive.

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

Accesso abusivo

Quali sono le fonti di rischio?

Personale operante, Soggetti terzi

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

Crittografia, Gestione postazioni, Sicurezza dell'hardware, Sicurezza dei canal informatici, Tracciabilità, Archiviazione, Archiviazione

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

Trascurabile, la gravità del rischio è trascurabile perché la modifica delle registrazioni di accesso e delle attività potrebbe essere eseguita soltanto dal designato o dalla ditta di manutenzione

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

Trascurabile,
Le misure di sicurezza a la mancata registrazione dei LOG rende improbabile accesso abusivo ai dati.

Valutazione : Accettabile

RISCHI

Perdita di dati

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

Perdita di registrazioni, Perdita di informazioni, impossibilità di tutelare un diritto

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

Danno hardware, Evento sismico, Incendio, Sabotaggio, Danno accidentale

Quali sono le fonti di rischio?

Personale operante, Soggetti terzi, Ambiente

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

Crittografia, Gestione postazioni, Sicurezza dell'hardware, Sicurezza dei canal informatici, Tracciabilità, Archiviazione, Archiviazione.

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

La gravità è limitata perché, sono state messe in atto misure di sicurezza che rendono improbabile la perdita di dati.

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

Trascurabile,
Trascurabile. La probabilità è trascurabile in quanto l'accesso ai dati è riservato e i dati sono registrati su server e protetti da sistemi di backup e firewall. E' prevista una modalità di manutenzione accessibile al solo personale di Digital PA s.r.l. attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Valutazione : Accettabile

* documento redatto in collaborazione con il DPO dell'Ente