Data Privacy Impact Assessment (DPIA)

Servizio SaaS per la Procedura per la segnalzione illeciti

ELENCO DELLE REVISIONI

REV.	DATA	NATURA DELLE MODIFICHE	APPROVAZIONE
01	20/02/2024	Prima Emissione	Titolare del trattamento

1. 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. 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.

2. Contesto

Il decreto legislativo 10 marzo 2023, n. 24 (in vigore dal 15 luglio 2023), recependo in Italia la direttiva UE 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, ha recato nuove disposizioni per la protezione delle persone che segnalano violazioni del diritto dell'Unione europea e delle disposizioni normative nazionali. Tale decreto raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti, sia del settore pubblico che privato.

Il whistleblower è la persona fisica che effettua la segnalazione di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo (non solo il dipendente della pubblica amministrazione, ma anche il lavoratore autonomo o il professionista o consulente che presta la propria attività presso il soggetto pubblico, la persona con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, il volontario e il tirocinante retribuito o non retribuito, e tutte le altre figure previste dal decreto, per le quali la tutela si applica anche durante il periodo di prova e anteriormente o successivamente alla costituzione del rapporto di lavoro o altro rapporto giuridico).

Il whistleblowing è la procedura a disposizione del lavoratore per segnalare eventuali condotte illecite che riscontra nell'ambito della propria attività lavorativa.

Il legislatore ha previsto importanti tutele per coloro che segnalano e ha obbligato le pubbliche amministrazioni a utilizzare modalità anche informatiche e strumenti di crittografia per garantire la riservatezza dell'identità del segnalante, del contenuto delle segnalazioni e della relativa documentazione.

A questi fini, il Comune di Bagno a Ripoli ha aderito al progetto "WhistleblowingPA" di Transparency International Italia e di Whistleblowing Solutions ed ha adottato la piattaforma informatica adesso prevista – quale canale di

segnalazione interna - per adempiere ai predetti obblighi normativi, ritenendo fondamentale dotare l'ente di uno strumento sicuro e di facile utilizzo per effettuare le segnalazioni in questione.

Le caratteristiche di questa nuova modalità di segnalazione sono le seguenti:

- la segnalazione viene fatta attraverso la compilazione di un questionario e può essere inviata in forma anonima. Se anonima, sarà presa in carico solo se adeguatamente circostanziata;
- la segnalazione viene ricevuta dal Responsabile per la Prevenzione della Corruzione e della Trasparenza (RPCT) e da lui gestita mantenendo il dovere di confidenzialità nei confronti del segnalante;
- nel momento dell'invio della segnalazione, il segnalante riceve un codice numerico di 16 cifre che deve conservare per poter accedere nuovamente alla segnalazione, verificare la risposta dell'RPCT e dialogare rispondendo a richieste di chiarimenti o approfondimenti;
- la segnalazione può essere fatta da qualsiasi dispositivo digitale (pc, tablet, smartphone) sia dall'interno dell'ente che dal suo esterno. La tutela dell'anonimato è garantita in ogni circostanza.

I soggetti che possono inviare segnalazioni di illecito o irregolarità amministrative sono:

- Dipendenti del Comune;
- Dipendenti di un ente di diritto privato sottoposto a controllo pubblico del Comune ai sensi del Codice Civile;
- Dipendenti delle società in house, degli organismi di diritto pubblico o dei concessionari di pubblico servizio;
- Lavoratori e collaboratori di imprese che forniscono beni e servizi al Comune o che realizzano opere in favore del Comune;
- Lavoratori autonomi o collaboratori, liberi professionisti e consulenti che svolgono la propria attività presso il Comune;
- Volontari e tirocinanti, retribuiti e non retribuiti;
- Persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza;
- Partecipanti alle procedure concorsuali e/o di selezione;
- Dipendenti in prova;
- Pensionati e altri soggetti il cui rapporto di lavoro col Comune sia cessato per qualunque motivo (dimissioni, licenziamento, distacco, comando, aspettativa, etc.).

Sono oggetto di segnalazione comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica. Rilevano a tal fine:

- illeciti amministrativi, contabili, civili o penali;
- misure ritorsive adottate nei confronti del segnalante.

NON possono essere oggetto di segnalazione: contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale del segnalante o della persona che ha sporto una denuncia all'Autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate.

2.1. Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi del D.lgs. n. 24/2023. La gestione delle segnalazioni viene effettuata attraverso un servizio esterno erogato in modalità SaaS da Transparency

International Italia e di Whistleblowing Solutions. Le misure tecniche di sicurezza dichiarate dal Fornitore e valutate dall'Ente sono riportate all'indirizzo https://www.whistleblowing.it/data/WBIT-documentazione-supporto-dpia.pdf . Tale documento è allegato alla presente DPIA e ne è parte integrante (di seguito DOC-MIS-WB).

2.2 Responsabilità connesse al trattamento

Ruolo	Nominativo
Titolare del trattamento	Comune di Bagno a Ripoli
Responsabile del trattamento	Whistleblowing Solutions I.S. S.r.l., con sede in Viale Abruzzi 13/A, 20131, Milano, Codice
Sub Responsabile	Transparency International Italia
Incaricati al trattamento	RPCT

2.3 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

2.4 Dati, processi e risorse di supporto

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
Dati personali comuni e di contatto	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Fornitori che effettuano una segnalazione o vengono segnalati
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 che effettuano una segnalazione o vengono segnalati
Dati giudiziari (es. condanne penali)	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Fornitori che effettuano una segnalazione o vengono segnalati

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

2.5. Risorse a supporto dei dati

Piattaforma Whistleblowing Solutions I.S. S.r.l. e Transparency International Italia

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.
Quali sono le basi giuridiche 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) 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 in quanto 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.

3.1. 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 attraverso la pubblicazione sito internet dell'Ente – 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 ai sensi degli, tramite piattaforma artt. 6.1. lett. a) e 7 del GDPR.
Come fanno gli interessati a esercitare i loro diritti previsti dagli artt. 15 ss. GDPR?	Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso l'indirizzo di posta elettronica dedicato responsabileprotezionedati@comune.bagno-a-ripoli.fi.it 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.

4. Misure esistenti

Le misure tecniche di sicurezza dichiarate dal Fornitore e valutate dall'Ente sono riportate in DOC-MIS-WB allegato alla presente DPIA.

5. Rischi

5.1 Metodologia

In riferimento alla procedura "Valutazione del Rischio_Trattamenti ad Alto rischio"

Come indicato dal considerando 76, il Comune si è dotato di un sistema di calcolo del rischio basato su **parametri oggettivi**, al fine di stabilire se esiste un rischio o un rischio elevato per il trattamento specifico. L'Oggettivazione del rischio pertanto passa attraverso un modello di creazione della probabilità e della Gravità in grado di rispecchiare il contesto in cui l'organizzazione opera. Sono state identificate griglie oggettive di calcolo delle Probabilità e Gravità con riguardo ai diritti e libertà dell'interessato.

Matrice Ri = P x G					
	Probabilità	1 - Trascurabile	2 – Limitata	3 – Importante	4 – Massima
Gravità	1 - Trascurabile	1	2	3	4
	2 – Limitata	2	4	6	8
	3 – Importante	3	6	9	12
	4 – Massima	4	8	12	16

Gravità	Significato	Descrizione generica degli impatti (diretti e indiretti)
4	Massima	I soggetti interessati possono incontrare conseguenze irreversibili.
3	Importante	I soggetti interessati possono incontrare conseguenze significative, e difficoltà nella loro risoluzione, ma comunque superabili.
2	Limitata	I soggetti interessati possono incontrare inconvenienti superabili.
1	Trascurabile	Gli interessati non saranno coinvolti o potrebbero incontrare alcuni lievi inconvenienti senz'altro superabili.

Probabilità	Significato	Criterio di scelta
4	Massima	Il verificarsi del danno dipende da condizioni direttamente connesse alla situazione; Il verificarsi del danno non provocherebbe alcuna reazione di stupore; Eventi simili sono già accaduti in azienda o in aziende dello stesso tipo
3	Importante	Il verificarsi del danno dipende da condizioni non direttamente connesse alla situazione ma possibili; Il verificarsi del danno provocherebbe reazioni di moderato stupore; Eventi simili sono stati già riscontrati
2	Limitata	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili si sono verificati molto raramente
1	Trascurabile	Il verificarsi del danno è subordinato a un concatenamento di eventi indipendenti tra loro; Il Verificarsi del danno è creduto impossibile dagli addetti; Non è mai accaduto nulla di simile

Valutazione della percentuale di abbattimento ottenibile con l'applicazione di contromisure

Rating	Tipologia di contromisura
1-25%	Non adeguata
26-50%	Minima
51-75%	Adeguata

Rating del Rischio residuo (Rr)

Rischio Alto	6,1-16
Rischio Medio	3,1-6
Rischio Basso	1-3

Elementi per la valutazione

a. **Ri** è il Rischio Inerente valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione
b. **Rr** è il Rischio Residuo calcolato al netto delle misure di mitigazione del rischio (determinate in via percentuale - % abbattimento)
c. Il Comune valuta come soglia di Rischio Accettabile (**Ra**) = **3**

5.1 Analisi dei rischi

5.1.1. Accesso illegittimo – Perdita della riservatezza

GRAVITÀ (G)	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.
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste del sistema o da attacco esterno. Non si hanno evidenze di accadimenti di questa tipologia di eventi sulla piattaforma SaaS
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)
MISURE	Le misure che contribuiscono a mitigare il rischio sono riportate in DOC-MIS-WB allegato alla presente DPIA. In particolare, si è valutato positivamente: ○ l'uso della crittografia, ○ l'uso del protocollo di doppia autenticazione degli utenti, ○ il fatto che l'applicativo GlobaLeaks 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. ○ Tutte le connessioni sono protette tramite protocollo TLS 1.2+ ○ I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, inaggiunta al sistema di allarme e barriere fisiche presidiate 7x24. ○ I datacenter del fornitore IaaS sono certificati ISO27001. ○ Sono presenti le seguenti certificazioni per la conformità normativa a standard internazionali: - ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks" - ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud - ISO27018 per la protezione dei dati personali nei servizi Public Cloud - Qualifica AGID - Certificazione CSA Star

CALCOLO DEL RISCHIO RESIDUO						
		G	**P**	**Ri**	**Mitigazione % abbattimento rischio**	**Rr**
		3	**2**	**6**	70%	**1,8**

5.1.2. Modifiche indesiderate – Perdita dell'integrità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, presenza di informazioni non corrette relative ai propri dati, lavorative.					
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste del sistema Non si hanno evidenze di accadimenti di questa tipologia di eventi sulla piattaforma SaaS					
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici.					
MISURE	Le misure che contribuiscono a mitigare il rischio sono riportate in DOC-MIS-WB allegato alla presente DPIA. In particolare, si è valutato positivamente la presenza di un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing .					
CALCOLO DEL RISCHIO RESIDUO						
		G	**P**	**Ri**	**Mitigazione % abbattimento rischio**	**Rr**
		3	**2**	**6**	70%	**1,8**

5.1.2. Perdita del dato – Perdita della disponibilità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Impossibilità di accedere alle proprie segnalazioni, impossibilità per l'Ente di trattare le segnalazioni ricevute

PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste del sistema. Non si hanno evidenze di accadimenti di questa tipologia di eventi sulla piattaforma SaaS
FONTI DI RISCHIO	Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici.
MISURE	Le misure che contribuiscono a mitigare il rischio sono riportate in DOC-MIS-WB allegato alla presente DPIA. In particolare, si è valutato positivamente l'implementazione di un sistema di High Availability e la presenza delle seguenti certificazioni per la conformità normativa a standard internazionali: - ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks" - ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud - ISO27018 per la protezione dei dati personali nei servizi Public Cloud - Qualifica AGID - Certificazione CSA Star
CALCOLO DEL RISCHIO RESIDUO	

	G	P	Ri	Mitigazione % abbattimento rischio	Rr
	3	2	6	70%	1,8

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

L'avv. Marco Giuri, in qualità di DPO del Comune di Bagno a Ripoli, ha espresso 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 inerenti (Ri)" con impatto sui diritti e libertà degli interessati con stima a valore Medio. Nell'ottica di mitigazione di tali rischi, si evince che, con l'implementazione delle misure tecnico/organizzative implementate dal Responsabile del Trattamento, il valore di rischio residuo rientra nei parametri accettabili uguali o minori rispetto al Rischio accettato (Ra) dall'organizzazione.

Si ritiene pertanto che il trattamento in oggetto presenta un grado di rischio sui diritti e libertà dell'interessato rientrante nei parametri accettabili e di conseguenza non è richiesta una consultazione preventiva all'Autorità Garante

9. Riferimenti

Valutazione d'impatto della protezione dei dati (DPIA) – Garante per la protezione dei dati personali:

https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-

Documentazione a supporto del titolare nella valutazione d'impatto sulla protezione dei dati - Whistleblowing Solutions I.S. S.r.l:

https://www.whistleblowing.it/data/WBIT-documentazione-supporto-dpia.pdf

10. Riferimenti

Si allegano alla presente Valutazione di impatto :

1. Documentazione a supporto del titolare nella valutazione d'impatto sulla protezione dei dati - Whistleblowing Solutions I.S. S.r.l:

2. Accordo in merito al trattamento dei dati personali tra Comune di Bagno a Ripoli e Whistleblowing Solutions I.S. s.r.l. (Nomina Responsabile del trattamento).

3. Accordo per il trattamento dei dati personali tra Whistleblowing Solutions Is e Transparency International Italia;

4. Accordo per il trattamento dei dati personali tra Whistleblowing Solutions Is e Seeweb srl.

5. Informativa Comune Bagno a Ripoli ai sensi dell'art. 13 Reg. UE 679/2016

6. Informativa WBPA ai sensi dell'art. 13 Reg. UE 679/2016