Allegato D

Comune di Rubano
Provincia di Padova

Valutazione di impatto sulla protezione dei dati personali ex art. 35 GDPR

1. DATI DEL TITOLARE E DEI RESPONSABILI DEL TRATTAMENTO

Titolare del trattamento	
Nome	**Comune di Rubano**
Indirizzo	Via A. Rossi, 11, 35030 Rubano (PD)
E-mail	protocollo@rubano.it
PEC	rubano.pd@cert.ip-veneto.net
Responsabile del trattamento	
Nome	**Whistleblowing Solutions Impresa Sociale S.r.l.**
Indirizzo	Viale Abruzzi 13/A, 20131, Milano
E-mail	info@whistleblowingsolutions.it
PEC	info@pec.whistleblowingsolutions.it
Parte del trattamento gestita	Fornitura e gestione del sistema di whistleblowing
Subresponsabili del trattamento	
Nome	**Seeweb S.r.l.**
Parte del trattamento gestita	Gestione dell'infrastruttura (IaaS)
Nome	**Transparency International Italia**
Parte del trattamento gestita	Collaborazione con il Responsabile nella gestione del sistema di whistleblowing
Data di completamento della Valutazione di impatto	
20 febbraio 2024	

2. NECESSITÀ DI UNA VALUTAZIONE DI IMPATTO EX ART. 35 GDPR

Il Decreto Legislativo n. 24 del 10 marzo 2023 di attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio ha modificato la disciplina in materia di whistleblowing, allargandone il relativo perimetro.

I "soggetti del settore pubblico", così come definiti all'art. 2, co. 1, lett. p) del citato Decreto, sono tenuti ad individuare opportuni canali di segnalazione interna, sentite le rappresentanze o le organizzazioni sindacali di cui all'art. 51 del d.lgs. n. 81/2015.

L'adozione di una piattaforma informatica per la raccolta e la trasmissione delle segnalazioni di c.d. whistleblowing comporta di dover considerare nuovi elementi rilevanti dal punto di vista della protezione dei dati personali, come precisato anche dalle Linee guida dell'ANAC del 12 luglio .

L'art. 13, co. 6 del D. lgs. 24/2023 prevede la necessità di individuare, relativamente al modello adottato di ricevimento e gestione delle segnalazioni interne, misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, "sulla base di una valutazione d'impatto sulla protezione dei dati".

Nello specifico, il Comune di Rubano (il "Comune") ha scelto di avvalersi del software gratuito "WhistleblowingPA" (la "Piattaforma") fornito da Transparency International Italia (organizzazione no profit) e da Whistleblowing Solutions Impresa Sociale S.r.l. Whistleblowing Solutions opera in qualità di Responsabile del trattamento ed è stata a tal fine appositamente nominata dal Comune. Whistleblowing Solutions, a propria volta, ha nominato Transparency International Italia (per il supporto alla gestione della Piattaforma) e Seeweb S.r.l. (per la fornitura di server, spazio cloud e servizio VPN, che compongono l'infrastruttura IAAS) quali Subresponsabili del trattamento e ha messo a disposizione del Comune le relative nomine che sono state nominate Responsabili del trattamento. La Piattaforma è stata realizzata per mezzo del software libero e open source GlobaLeaks. La Piattaforma specifica per il Comune è resa disponibile in cloud, ad un indirizzo internet dedicato.

La Piattaforma non richiede servizi di manutenzione né interventi tecnici da parte di soggetti interni o esterni al Comune.

Il Comune prevede che le segnalazioni dovranno essere preferibilmente inoltrate tramite detta Piattaforma.

La Piattaforma permette l'invio di comunicazioni da parte di soggetti segnalanti appartenenti alle categorie indicate all'art. 3, co. 3 e 4 del D. lgs. 24/2023 e quindi da parte di:

a) dipendenti del Comune assunti a tempo determinato e indeterminato;

b) collaboratori, fornitori e subfornitori e loro dipendenti, liberi professionisti, consulenti, volontari e tirocinanti (retribuiti o non retribuiti) che a qualsiasi titolo prestano la propria attività presso il Comune, ivi compresi i lavoratori autonomi indicati al capo I della legge 81/2017, nonché i titolari di rapporto di collaborazione di cui all'art. 409 c.p.c.;

c) persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora esercitate in via di mero fatto, presso il Comune;

d) ex dipendenti, ex collaboratori o persone che non ricoprono più una delle posizioni indicate in precedenza;

e) soggetti in fase di selezione, di prova o il cui rapporto giuridico con l'ente non sia ancora iniziato.

Le comunicazioni inoltrate tramite la Piattaforma devono avere ad oggetto una segnalazione di una violazione di leggi nazionali o europee, che il segnalante ritiene fondatamente e in buona fede che sia avvenuta. Il Comune prevede la segnalazione di comportamenti, atti od omissioni commessi o che, sulla base di elementi concreti, si ritiene potrebbero essere commessi all'interno del Comune, nonché eventuali condotte volte ad occultare tali violazioni, che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica e consistenti in:
- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del D. lgs. 231/2001;
- tutte le ulteriori tipologie di illeciti che rientrano nell'ambito di applicazione dell'art. 2, comma 1, lett. a), nn. 3, 4, 5 e 6 del D. lgs. 24/2023.

3. INTRODUZIONE NORMATIVA E SISTEMI DI VALUTAZIONE DEL RISCHIO

La valutazione di impatto ("DPIA") viene definita nel dettaglio dal Comitato Europeo per la protezione dei dati[1] (CEPD o EDPB, ex WP29), che la identifica come "*un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità*".

Ai sensi dell'art. 35 del Regolamento UE 2016/679 ("GDPR"), la valutazione di impatto deve contenere almeno:

"a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione."

L'art. 35 del GDPR stabilisce che, quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato

1 Il comitato europeo per la protezione dei dati è un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE.
Il Comitato europeo per la protezione dei dati è composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (GEPD). Ne fanno altresì parte le autorità di controllo degli Stati EFTA/SEE per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati (GDPR).

per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Inoltre, il medesimo articolo stabilisce che la valutazione di impatto è obbligatoria qualora avvenga:

"a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico."

Tuttavia, è bene specificare che il semplice fatto che le condizioni che comportano l'obbligo di realizzare una valutazione d'impatto sulla protezione dei dati non siano soddisfatte non diminuisce l'obbligo generale, cui i titolari del trattamento sono soggetti, di attuare misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli interessati. In pratica, ciò significa che i titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Invero, i trattamenti elencati dall'art. 35 GDPR paragrafo 3, che comportano obbligatoriamente l'adozione di una valutazione di impatto, rappresentano un'elencazione non esaustiva di tutti i trattamenti necessitanti di detta valutazione. Vi possono infatti essere operazioni che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto "elevati" e che devono quindi essere sottoposti ad una valutazione d'impatto.

Nel 2017 l'EDPB ha adottato delle Linee guida sulla DPIA in cui ha ulteriormente specificato alcune ipotesi in cui la stessa è ritenuta necessaria. Ne è infatti consigliata l'adozione qualora sussistano almeno due delle ipotesi indicate. Su questo modello, anche il Garante italiano, con proprio provvedimento dell'11 ottobre 2018, ha poi predisposto un elenco - comunque non esaustivo - delle tipologie di trattamento ai sensi dell'art. 35, par. 4 che devono essere necessariamente sottoposte a valutazione d'impatto.

È bene evidenziare infine che la consultazione dell'Autorità Garante in via preventiva rispetto al trattamento è necessaria, ai sensi dell'interpretazione più diffusa dell'articolo 36 GDPR, solo qualora la valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati.

La responsabilità per l'implementazione e l'adozione della DPIA è in capo al Titolare del trattamento, a cui spetta garantire l'effettuazione della stessa, sebbene la conduzione materiale possa essere affidata ad un altro soggetto, interno o esterno all'organizzazione aziendale. Il Titolare deve consultarsi con il DPO, ove presente. Qualora risulti che il trattamento sia svolto in tutto o in parte da un Responsabile del trattamento, quest'ultimo deve assistere il Titolare nella conduzione della DPIA, fornendo ogni informazione necessaria.

4. DESCRIZIONE DEL TRATTAMENTO

4.1 DATI TRATTATI E CATEGORIE DI INTERESSATI

La Piattaforma tratta dati personali che vengono comunicati da diverse tipologie di utenti.

Soggetti interessati	**Dati trattati**
Responsabile della gestione del canale di segnalazione (individuato dal Comune nel Responsabile per la Prevenzione della Corruzione e la Trasparenza – RPCT)	Dati richiesti in fase di registrazione (nome, cognome, indirizzo e-mail, dati contenuti nei log tracciati dalla Piattaforma)
Segnalanti	Dati richiesti in fase di registrazione (nel caso di segnalazione non anonima: nome, cognome, data di nascita, codice fiscale, qualifica, mansione lavorativa, facoltativo indirizzo e-mail o PEC); dati contenuti nelle segnalazioni inviate, inclusi eventuali dati appartenenti a categorie particolari o dati relativi a condanne penali o reati; dati comunicati tramite il servizio di messaggistica

	della Piattaforma
Persone segnalate	Dati contenuti nelle segnalazioni
Soggetti terzi (accusato, persona informata sui fatti, testimoni ecc.)	Dati contenuti nelle segnalazioni

4.2 CONTESTO DEL TRATTAMENTO

Il Comune di Rubano è un comune italiano di 16.938 abitanti circa, con le sue frazioni di Bosco, Sarmeola e Villaguattera, si trova in una posizione strategica a livello territoriale nella provincia di Padova, sviluppandosi lungo la Strada Regionale 11; ha una superfice di 14,6 kmq.

Il Comune è dotato di due Organi di governo, la Giunta comunale e il Consiglio comunale, e la struttura organizzativa prevede cinque Aree; ciascuna Area ricomprende diversi Uffici al proprio interno.

Le Aree, così come descritti nella sezione "Amministrazione trasparente" del sito istituzionale (Amministrazione trasparente), sono le seguenti: Economico-finanziara; Risorse Umane e Servizi Informatici; Segreteria, Contratti, PuntoSi, cultura; Servizi alla Persona; Gestione del Territorio, Pianificazione del Territorio.

Il Responsabile della gestione del canale di segnalazione è stato individuato nel Responsabile per la Prevenzione della Corruzione e la Trasparenza (RPCT), in conformità a quanto previsto dall'art. 4, co. 5 del D. lgs. 24/2023.

4.3 FLUSSO DEI DATI

Il segnalante accede alla Piattaforma per le segnalazioni tramite apposito link pubblicato sul sito istituzionale del Comune.

Il segnalante dovrà quindi indicare se intenda effettuare una nuova segnalazione oppure accedere a una segnalazione già presentata (mediante un codice).

Il segnalante inserisce quindi nel form apposito le informazioni relative alla segnalazione, eventuali documenti a supporto e, ove lo desideri, i propri dati identificativi.

Il segnalante accede quindi all'informativa privacy e deve confermare di averne preso visione. Al termine della compilazione, dopo aver verificato la correttezza e completezza delle informazioni conferite, il segnalante deve cliccare sul tasto "invia" per trasmettere definitivamente la segnalazione, che verrà acquisita e registrata dalla Piattaforma.

Al termine della procedura di segnalazione, la Piattaforma restituisce come ricevuta un codice di 16 cifre, che rappresenta l'unico mezzo per accedere alla segnalazione.

Per accedere all'area riservata e visualizzare la segnalazione trasmessa, è sufficiente per il segnalante premere il tasto "vedi la tua segnalazione" oppure collegarsi alla homepage, inserendo il codice e premendo il tasto "accedi".

All'interno dell'area riservata, il segnalante può caricare ulteriore documentazione e/o integrare la segnalazione compilando la sezione "commenti" o interagendo con il Responsabile delle segnalazioni.

La Piattaforma è composta da un'infrastruttura privata Infrastructure as a Service (IAAS) e Software as a Service (SAAS) ed è accessibile tramite la rete internet mediante protocollo HTTPS. La Piattaforma poggia su server dedicati e certificati, messi a disposizione da Seeweb e localizzati all'interno dell'Unione Europea.

Il Comune ha individuato come canale preferenziale l'utilizzo della Piattaforma, pertanto, ove il segnalante decidesse di ricorrere a diversi mezzi di comunicazione, la riservatezza sua e del contenuto della segnalazione saranno garantiti dalle ordinarie misure di sicurezza tecniche e organizzative applicabili allo strumento scelto.

4.4 TIPOLOGIA DI DATI TRATTATI E BASI GIURIDICHE

Il Titolare del trattamento tratta i dati personali sopra individuati sulla base di un obbligo di legge cui è soggetto (art. 6.1, lett. c) GDPR) e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6.1, lett. e) GDPR, in conformità all'art. 2ter del D. lgs. 30 giugno 2003, n. 196 ("Codice privacy") e al D. lgs. 24/2023).

È necessario, invece, il consenso del segnalante per rivelarne l'identità (art. 6.1, lett. a) GDPR), fatti i salvi i casi in cui detta rivelazione sia prevista per legge.

Il Titolare del trattamento è consapevole del fatto che, mediante le segnalazioni, potrebbe venire a conoscenza anche di dati relativi a condanne penali o reati, o di dati appartenenti a categorie particolari, ai sensi degli artt. 10 e 9 GDPR. Tali dati saranno in ogni caso trattati solo dai Responsabili delle segnalazioni, per le finalità previste per legge e quindi, per i dati particolari, in conformità all'art. 9.2, lett. b) o g) GDPR (obbligo di legge in materia di diritto del lavoro, protezione o sicurezza sociale ed esecuzione di un interesse pubblico rilevante, in connessione con l'art. 2-sexies, comma 2, lett. dd), del Codice privacy); per i dati relativi a condanne penali o reati, in conformità agli artt. 10 GDPR e 2octies del Codice privacy.

4.5 FINALITÀ DEL TRATTAMENTO E IMPATTO SUGLI INTERESSATI

Da quanto in precedenza esposto, risulta che la finalità del trattamento dei dati personali è rappresentata dalla necessità di creare e gestire i canali di segnalazione interni in conformità a quanto previsto dal D. lgs. 24/2023 e documentare l'attività svolta per tutelare l'interesse pubblico e l'integrità del Comune, mediante la prevenzione e repressione di reati. Al contempo, i dati personali sono trattati tenendo in considerazione la necessità di tutelare la riservatezza dei segnalanti.

Il trattamento operato, in ultima analisi, porta benefici a tutte le diverse categorie di interessati, perché garantisce modalità sicure di supporto per il Responsabile delle segnalazioni e protezione ai segnalanti. In questo modo, il Titolare del trattamento può adempiere in modo più efficiente alle obbligazioni che gli derivano per legge e dal rapporto istituito con gli interessati. Si ritiene altresì che, in considerazione delle misure di sicurezza tecniche e organizzative implementate, il trattamento di dati personali operato tramite un canale preferenziale come la Piattaforma risulta maggiormente tutelante per gli interessati rispetto ad altri mezzi di comunicazione e non comporta la raccolta di dati né eccessivi né sproporzionati.

4.6 CONSERVAZIONE DEI DATI

I dati degli interessati raccolti in sede di registrazione e per l'invio delle segnalazioni sono conservati per 12 mesi, a meno che il segnalante, per propria scelta, o il Responsabile delle segnalazioni, nel rispetto della legge e delle procedure adottate dal Comune, non ne richiedano la cancellazione anticipatamente.

Il tempo di conservazione può essere prorogato dietro indicazione del Responsabile delle segnalazioni.

Le segnalazioni e i dati ad esse correlati non saranno conservati oltre cinque anni dalla data della comunicazione al segnalante dell'esito finale della procedura di segnalazione. Nel caso di contenzioso o di segnalazione all'Autorità giudiziaria o ad ANAC, il trattamento potrà essere protratto anche oltre i termini sopra indicati, fino al termine di decadenza di eventuali ricorsi e fino alla scadenza dei termini di prescrizione per l'esercizio dei diritti e/o per l'adempimento di altri obblighi di legge.

5. PROCESSO DI CONSULTAZIONE

L'art. 35.9 GDPR prevede che il Titolare del trattamento debba valutare l'opportunità di raccogliere "le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti."

A tale riguardo, si specifica che la consultazione degli interessati al momento non è stata ritenuta necessaria in quanto il Titolare del trattamento agisce in esecuzione e in conformità a obblighi di legge, che trovano dettagliata disciplina, anche per mezzo delle specifiche Linee Guida ANAC adottate. Pertanto, si ritiene che gli interessati siano già sufficientemente informati e le loro opinioni rappresentate.

Gli interessati, peraltro, appartengono a svariate categorie non sempre rappresentate. Tuttavia, come previsto dalla normativa, il Titolare del trattamento ha informato le rappresentanze sindacali dell'adozione della Piattaforma e delle procedure di segnalazione.

6. PRINCIPI FONDAMENTALI

Il GDPR indica quali sono i principi fondamentali che devono in ogni caso essere seguiti nello svolgimento delle attività e dei trattamenti dei dati personali raccolti.

a. Principio di liceità: i trattamenti di dati personali devono necessariamente avere una base giuridica ed essere conformi alle norme dell'ordinamento giuridico.
b. Principio di correttezza: i dati personali devono essere trattati secondo buona fede.
c. Principio di trasparenza: devono essere facilmente accessibili e comprensibili le informazioni e le comunicazioni relative le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i dati personali e deve essere utilizzato un linguaggio semplice e chiaro.
d. Principio di limitazione delle finalità: i dati devono essere raccolti per finalità legittime ed individuate fin dall'inizio, e successivamente trattati in modo che non sia incompatibile con tali finalità. Nello specifico, i dati personali devono essere raccolti solo al fine di gestire e dare seguito alle segnalazioni, divulgazioni pubbliche o denunce effettuate da parte dei soggetti tutelati dal D. lgs. 24/2023.
e. Principio di esattezza dei dati: i dati devono essere corretti e, se necessario, aggiornati, con conseguente obbligo di cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati. Devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti relativi alla specifica segnalazione, divulgazione pubblica o denuncia che viene gestita. I segnalanti stessi possono modificare e correggere i dati condivisi con le segnalazioni accedendo all'area riservata.
f. Principio di limitazione della conservazione: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per il tempo strettamente necessario al conseguimento delle finalità per le quali sono trattati e quindi per la gestione della specifica segnalazione, e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.
g. Principio di integrità e riservatezza: i dati devono essere trattati mediante l'adozione delle misure tecniche ed organizzative idonee ad assicurarne la sicurezza rispetto a trattamenti non autorizzati o illeciti e alla perdita, distruzione o danno accidentali.
h. Principio di minimizzazione: i dati trattati devono essere solamente quelli indispensabili, quindi pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. A tale riguardo, il D. lgs. 24/2023 precisa che i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati senza indugio. Nel rispetto del principio di privacy by design, tutti i dispositivi utilizzati dal Responsabile del trattamento quali applicativo GlobaLeaks, log di sistema e firewall, sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante.
i. Principio di responsabilizzazione: compete al Titolare del trattamento l'identificazione di adeguate garanzie per tutelare i diritti e le libertà degli interessati e la documentazione dell'avvenuta adozione delle stesse.

I principi fondamentali qui menzionati devono guidare il Titolare del trattamento nello sviluppo e nell'implementazione del progetto e devono fungere da linee guida per l'individuazione delle misure di sicurezza più adatte a garantire un'adeguata protezione dei dati trattati e dei diritti e libertà degli interessati.

Nel caso del trattamento qui descritto, come si vedrà nei paragrafi a seguire, il Comune ha pienamente rispettato questi principi sia nella fase di progettazione dei trattamenti sia nella fase di individuazione delle misure di sicurezza più idonee a consentire la limitazione dei rischi connessi ai trattamenti.

7. NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO (ART. 35.7, LETT. B))

7.1 VALUTAZIONE DELLA NECESSITÀ E PROPORZIONALITÀ

Il Comune è consapevole che il trattamento di dati personali che avviene attraverso la Piattaforma potrebbe incidere sui diritti e le libertà degli interessati, a cominciare dal diritto alla riservatezza della vita privata, che potrebbe essere leso da un trattamento illegittimo per la sua configurazione o modalità di attuazione.

Il trattamento di dati personali effettuato dal Comune, tuttavia, risulta necessario per il perseguimento delle finalità stabilite per legge e lo stesso è eseguito mediante modalità che garantiscono la sicurezza e la riservatezza previste dalla stessa normativa.

In secondo luogo, il trattamento dei dati personali risulta proporzionato rispetto alle finalità perseguite. Il Comune, infatti, tratta solo i dati necessari e rilevanti per le finalità prestabilite, in conformità all'art. 5 GDPR. Inoltre, il Comune ha valutato che non esistano strumenti e mezzi per ottenere le stesse finalità, con un minore impatto sugli interessati.

Infine, la qualità e l'integrità dei dati, oltre alla loro minimizzazione, viene garantita dal Comune per mezzo dell'adozione delle misure di sicurezza di cui si darà atto nei paragrafi seguenti.

7.2 MISURE DI PROTEZIONE DEI DIRITTI DEGLI INTERESSATI

In particolare, al fine di limitare l'impatto sui diritti e le libertà degli interessati, il Comune intende adottare le seguenti misure:

i. adozione di specifiche informative privacy e procedure interne e aggiornamento del Codice di comportamento dei dipendenti comunali, per informare gli interessati in merito ai loro diritti, alle relative limitazioni e alle modalità di esercizio;
ii. atto di nomina ad autorizzato del trattamento ex art. 29 GDPR, riportanti le istruzioni impartite dal Titolare del trattamento, per il soggetto nominato Responsabile delle segnalazioni;
iii. assenza di trasferimenti di dati personali verso Paesi terzi;
iv. adozione di contratti di nomina dettagliati con tutti i Responsabili del trattamento coinvolti;
v. acquisizione del consenso degli interessati che, ove richiesto, viene prestato in modo specifico, esplicito, libero e previa consegna di adeguata informativa. Il consenso potrà essere prestato mediante sistemi automatici previsti all'interno della Piattaforma oppure verrà tracciato con documenti cartacei predisposti dal Comune;
vi. garanzia dell'esercizio dei diritti degli interessati previsti dagli artt. 15-22 GDPR, fatta eccezione per alcune limitazioni previste per legge ai sensi del combinato disposto dell'art. 13 del D. lgs. 24/2023 e dell'art. 2undecies del Codice privacy, di cui gli interessati vengono comunque informati. Le limitazioni dei diritti si applicano in particolare per i soggetti segnalati o menzionati nelle segnalazioni.

È quindi possibile affermare che il trattamento risulta necessario e proporzionato e non incide sul contenuto essenziale dei diritti degli interessati.

8. VALUTAZIONE DEL SISTEMA

Misure esistenti o pianificate

Crittografia

I dati sono gestiti mediante un'apposita piattaforma attivata dal Comune basata sul riuso del software GlobalLeaks, 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 previsto dalle Linee Guida Anac. GlobalLeaks è un software open-source creato per permettere l'avvio di iniziative di whistleblowing sicuro ed anonimo rilasciato sotto licenza AGPL (Affero General Public License). 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

• 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, Vandalismo

- 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.

- 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.

Valutazione : Accettabile

9. CONCLUSIONI

Dall'analisi delle misure di sicurezza organizzative e tecniche implementate dal Titolare del trattamento, è risultato che il rischio residuo è stato ridotto ad un livello accettabile e per tale ragione non si è ritenuto necessario procedere alla consultazione preventiva del Garante Privacy, altrimenti prevista dall'art. 36 del GDPR.

Ai sensi e per gli effetti del combinato disposto degli artt. 35, par. 2 e 39, par. 1, lett. c) del GDPR, a seguito della redazione dei precedenti paragrafi gli stessi sono stati trasmessi al Responsabile della protezione dei dati personali del Comune , il quale ha formulato parere positivo e ha confermato che il trattamento può essere avviato.

In relazione a tale parere, il Titolare del trattamento concorda con le indicazioni fornite dal Responsabile della protezione dei dati personali.

Si dà comunque atto, in conclusione, che il Comune si impegna a revisionare la presente valutazione di impatto al fine di attestare l'implementazione di eventuali ulteriori misure di sicurezza, adeguate e aggiornate rispetto allo stato della tecnica, e di dare atto delle modifiche eventualmente introdotte nel trattamento qui descritto, per scelta del Comune o per la necessità di adempiere a nuove previsioni normative.