VALUTAZIONE D'IMPATTO
SULLA PROTEZIONE DEI DATI PERSONALI
 # 1/2023

OGGETTO: SISTEMA DI GESTIONE DELLE SEGNALAZIONI DI VIOLAZIONI DI DISPOSIZIONI NORMATIVE NAZIONALI O DELL'UNIONE EUROPEA CHE LEDONO L'INTERESSE PUBBLICO O L'INTEGRITÀ DELL'AMMINISTRAZIONE PUBBLICA O DELL'ENTE PRIVATO, DI CUI IL SEGNALANTE SIA VENUTO A CONOSCENZA IN UN CONTESTO LAVORATIVO PUBBLICO O PRIVATO (WHISTLEBLOWING)

DATA DI CREAZIONE: Dicembre 2023

AUTORI: La DPIA è stata svolta dal Segretario generale, dott. Mario Ruggieri, designato e delegato dal Titolare del Trattamento, in qualità di Responsabile della prevenzione della corruzione e della trasparenza (RPCT) e dal Responsabile del Servizio Sistemi Informativi, dott. Paolo Scarabottini, previo parere del Responsabile Protezione dati, avv. Francesca Potì.

SEZIONE I

1. Oggetto

La presente valutazione d'impatto sulla protezione dei dati ha ad oggetto i trattamenti di dati personali effettuati dal Comune di Spoleto (il "**Comune**") nell'ambito della gestione del canale di segnalazione cd. interna implementato conformemente al D. Lgs. n. 24 del 10 marzo 2023.
Le operazioni di trattamento di dati personali includono quelle effettuate: (i) in fase di acquisizione delle segnalazioni; (ii) in fase di istruzione delle segnalazioni; (iii) in fase di utilizzo delle segnalazioni; (iv) in fase di conservazione delle segnalazioni.
La presente valutazione d'impatto non ha ad oggetto le operazioni di trattamento effettuate, in qualità di autonomi titolari del trattamento, da parte dell'Autorità Nazionale Anti Corruzione (ANAC), dell'autorità giudiziaria e dagli altri soggetti, diversi dai responsabili del trattamento, ai quali i dati possono essere comunicati.

2. Riferimenti normativi e metodologici

2.1. Nel prosieguo del presente documento, s'intende:
(a) per "**GDPR**", il 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;
(b) per "**Codice Privacy**", il Decreto legislativo n. 196 del 30 giugno 2003;
(c) per "**Decreto Whistleblowing**", il Decreto legislativo n. 24 del 10 marzo 2023;
(d) per "**categorie particolari di dati personali**", i dati che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale", nonché i "dati genetici", i "dati

biometrici intesi a identificare in modo univoco una persona fisica", i "dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (Art. 9, comma 1 GDPR);
(e) per "**dati giudiziari**", si intendono "i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza";
(f) per "**Gestore**", si intende la persona, l'ufficio interno autonomo dedicato e provvisto di personale specificamente formato, ovvero il soggetto esterno, autonomo e con personale specificamente formato, cui è affidata la gestione del canale di segnalazione. I soggetti del settore pubblico, ivi compresi gli Enti locali cui sia fatto obbligo di prevedere la figura del Responsabile della prevenzione della corruzione e della trasparenza - RPCT, di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, affidano a quest'ultimo la gestione del canale di segnalazione interna, eventualmente coadiuvato da un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del suddetto canale interno di segnalazione (cfr. articolo 4 commi 2 e 5 del Decreto Legislativo n. 24/2023);
(g) per "Procedura per la gestione delle segnalazioni trasmesse al Comune di Spoleto" si intende la procedura di gestione delle segnalazioni contenuta nel Piano Integrato di Attività e Organizzazione adottato dall'Ente disponibile sul sito istituzionale (www.comune.spoleto.pg.it) nella sezione "Amministrazione_trasparente/Disposizioni_generali/Atti_generali/Documenti_di_programmazione_strategico_gestionali".
2.2. Nella valutazione della sussistenza dei presupposti per lo svolgimento della valutazione d'impatto e nell'espletamento della medesima, sotto il profilo normativo, si è tenuto conto:
(i) degli artt. 35 e 36 del GDPR;
(ii) dei considerando nn. 75, 84, 89 e 90 del GDPR;
(iii) degli artt. 5, 6, 7, 12 – 22, 24, 25, 32, 35 e 88 del GDPR;
(iv) degli artt. 12, 13, 14 e 15 del Decreto Whistleblowing;
(v) del provvedimento n. 467 dell'11 ottobre 2018 del Garante per la Protezione dei Dati Personali e del relativo Allegato 1 ("*Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto*");
(vi) dei provvedimenti nn. 215 del 4 dicembre 2019 ("*Parere sullo schema di "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs. 165/2001 (c.d. whistleblowing)*"), 235 del 10 giugno 2021, 236 del 10 giugno 2021, 134 del 7 aprile 2022, 135 del 7 aprile 2022, 268 del 21 luglio 2022, 269 del 21 luglio 2022;
(vii) delle "*Guidelines on processing personal information within a whistleblowing procedure*" dello *European Data Protection Supervisor* (EDPS) del dicembre 2019.

2.3. Nell'elaborazione della valutazione d'impatto, sotto il profilo metodologico ed operativo, si è tenuto conto:
- delle Linee Guida n.248 rev.01 del WP 29 in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679;
- delle Linee Guida n.243 rev.01 del WP 29 sui responsabili della protezione dei dati emendata in data 5 aprile 2017;
- del *framework* predisposto dalla *Commission nationale de l'informatique et des libertés* (CNIL);
- delle Linee Guida ANAC in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali approvate con Delibera n. 311 del 12 luglio 2023.

3. Presupposti e ragioni dell'espletamento della valutazione d'impatto

Il trattamento dei dati personali effettuato mediante i sistemi di acquisizione gestione delle segnalazioni presenta rischi specifici per i diritti e le libertà degli interessati, considerata: *(i)* la particolare delicatezza delle informazioni potenzialmente trattate, *(ii)* la "vulnerabilità" degli interessati nel contesto lavorativo, *(iii)* lo specifico regime di riservatezza dell'identità del segnalante previsto dalla normativa di settore.
Come chiarito di recente dal Garante per la Protezione dei Dati Personali proprio con riferimento ai trattamenti effettuati mediante applicativi per l'acquisizione e gestione delle segnalazioni illecite, il trattamento dei dati personali effettuati in tale ambito presenta rischi specifici per i diritti e le libertà degli interessati e deve dunque essere sottoposto a valutazione di impatto ex art. 35 GDPR. Questo in ragione della particolare delicatezza delle informazioni trattate, nonché degli elevati rischi, in termini di possibili effetti ritorsivi e discriminatori, anche indiretti, per il segnalante, la cui identità è protetta da uno specifico regime di garanzia e riservatezza previsto dalla normativa di settore (tanto a livello nazionale quanto a livello europeo: cfr., da ultimo, la 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).
A ciò si aggiunga che l'art. 13, comma 6 del Decreto Whistleblowing subordina ad apposita valutazione d'impatto l'adozione di idonee misure dirette a garantire la sicurezza dei canali di segnalazione: "*I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando 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****, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018*".
La presente valutazione d'impatto viene pertanto espletata poiché il trattamento preso in considerazione rientra tra i *"trattamenti non occasionali di dati relativi a soggetti vulnerabili…*" (cfr. il punto 6 dell'Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018 del Garante per la Protezione dei Dati Personali, col quale è stato definito l'"*Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto*" conformemente a quanto previsto dagli artt. 35, co. 4, e 57, co. 1, lett. k), del GPDR, nonché il provvedimento n. 235 del 10 giugno 2021), e poiché espressamente previsto dall'art. 13, comma 6 del Decreto Whistleblowing.

SEZIONE II

4. Valutazione d'impatto

4.1 Descrizione sistematica del trattamento e ciclo di vita del trattamento dei dati

Le operazioni di trattamento oggetto di valutazione hanno ad oggetto l'acquisizione, la gestione e la conservazione delle segnalazioni di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui il segnalante sia venuto a conoscenza in un contesto lavorativo pubblico o privato, mediante i canali all'uopo implementati dal Comune.
Le operazioni di trattamento sono articolate nelle seguenti fasi:

(i) La fase di ricevimento delle segnalazioni ha luogo esclusivamente su iniziativa del segnalante, il quale può trasmettere la propria segnalazione impiegando distinti canali: *a)* tramite piattaforma informatica, con le modalità indicate in apposita sezione del sito web del Comune di Spoleto; *b)* in busta chiusa, attraverso il protocollo generale dell'Ente, avendo cura di precisare, all'esterno del plico cartaceo (che non dovrà contenere le generalità del segnalante), che trattasi di segnalazione "*whistleblowing – riservata*". In particolare, il segnalante dovrà predisporre differenti buste chiuse: la prima con i propri dati identificativi unitamente alla fotocopia del documento di riconoscimento; la seconda con l'esposizione del fatto segnalato, adeguatamente descritto e circostanziato. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all'esterno la dicitura "*riservata al RPCT*"). In mancanza di tali specifiche indicazioni non potranno essere assicurate le tutele del segnalante. Nel caso di impiego del plico cartaceo si procede con un protocollo riservato; c) la segnalazione può essere anche presentata oralmente; in tal caso il RPCT provvede a registrare o comunque a verbalizzare il colloquio con il segnalante, avvenuto tramite collegamento telefonico, telematico o incontro in presenza fissato entro un termine ragionevole.
Coloro che, in ragione del proprio rapporto di lavoro presso l'Ente, vengano a conoscenza di condotte illecite inviano la segnalazione all'Ente secondo la modalità di trasmissione prescelta. La segnalazione deve contenere: le generalità del soggetto che effettua la segnalazione, con indicazione della posizione o funzione svolta nell'ambito dell'ente; una chiara e completa descrizione dei fatti oggetto di segnalazione; le circostanze di tempo e di luogo in cui si sono verificati i fatti oggetto di segnalazione; le generalità o gli altri elementi che consentano di identificare il/i soggetto/i che ha/hanno posto in essere i fatti segnalati o a cui attribuire i fatti oggetto di segnalazione; l'indicazione di eventuali altri soggetti che possano riferire sui fatti oggetto di segnalazione; l'indicazione di documenti a supporto della segnalazione che possano confermare la fondatezza di tali fatti; ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.
Il Gestore della segnalazione è il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT). Qualora il RPCT (Segretario Generale dell'Ente) versi in situazioni di conflitto di interesse rispetto alla segnalazione ricevuta, la stessa verrà gestita dal Vice Segretario Generale dell'Ente. Il Gestore è tenuto a: (a) rilasciare al segnalante un avviso di ricevimento della segnalazione, entro 7 giorni dalla data di ricezione; (b) mantenere le interlocuzioni con il segnalante e chiedergli le eventuali integrazioni che risultino necessarie, dando diligente seguito alle segnalazioni ricevute; (c) fornire riscontro entro tre mesi data dell'avviso di ricevimento o, in mancanza di tale avviso, tre mesi dalla scadenza del termine di sette giorni presentazione della segnalazione.

Il segnalante può rivelare la propria identità oppure rimanere anonimo. Qualora il segnalante abbia rivelato la propria identità, anche successivamente, le informazioni anagrafiche sono conosciute esclusivamente dal Gestore e segregate rispetto al contenuto della segnalazione (in caso di utilizzo della piattaforma informatica, il software rilascia un "codice segnalazione" univoco che consente il tracciamento della segnalazione da parte del segnalante). Qualora il segnalante decida di non rivelare la propria identità, la segnalazione viene comunque istruita e trattata, a condizione che essa risulti sufficientemente circostanziata.

(ii) la seconda fase di istruzione delle segnalazioni costituisce una prima imparziale delibazione sulla sussistenza di quanto rappresentato nella segnalazione. Per lo svolgimento dell'istruttoria il RPCT può avviare un dialogo con il whistleblower, chiedendo allo stesso chiarimenti, documenti e informazioni ulteriori, tramite il canale della piattaforma informatica o anche di persona. Ove necessario, può anche acquisire atti e documenti da altri uffici dell'Ente, avvalersi del loro supporto, coinvolgere terze persone, tramite audizioni e altre richieste, avendo sempre cura che non sia compromessa la tutela della riservatezza del segnalante, quindi

trattando rigorosamente in maniera separata il contenuto della segnalazione rispetto all'identità del segnalante.

(iii) la terza fase comporta l'adozione, da parte dell'ente, dei provvedimenti conseguenziali all'esito dell'attività istruttoria. In particolare, qualora, a seguito dell'attività svolta, il RPCT ravvisi elementi di manifesta infondatezza della segnalazione, ne dispone l'archiviazione con adeguata motivazione. Qualora invece il RPCT ravvisi il fumus di fondatezza della segnalazione, si rivolgerà immediatamente ai seguenti organi preposti interni o enti/istituzioni esterne, ognuno secondo le proprie competenze, trasmettendo una relazione di risultanze istruttorie riferendo circa le attività svolte, per il prosieguo della gestione della segnalazione, avendo sempre cura di tutelare la riservatezza dell'identità del segnalante:
• il dirigente dell'Area in cui si è verificato il fatto, se non coinvolto nei fatti segnalati, per l'acquisizione di elementi istruttori, solo laddove non vi siano ipotesi di reato;
• l'ufficio procedimenti disciplinari, per eventuali profili di responsabilità disciplinare di competenza di quest'ultimo;
• l'Autorità Giudiziaria, la Corte dei conti e l'A.N.A.C., per i profili di rispettiva competenza;
• il Dipartimento della Funzione Pubblica.
Il RPCT allega a tale relazione la documentazione che ritiene necessaria espungendo tutti i riferimenti che possano consentire di risalire all'identità del segnalante.
Resta fermo che gli organi riceventi da quel momento sono titolari del trattamento dei dati.
Non spetta, invece, al RPCT accertare le responsabilità individuali qualunque natura esse abbiano né svolgere controlli di legittimità o di merito su atti e provvedimenti adottati dall'amministrazione oggetto di segnalazione.
(iv) la quarta fase, di archiviazione e conservazione delle segnalazioni, ha luogo a partire dal ricevimento della segnalazione e si conclude fino ad un periodo massimo di cinque anni dalla definizione della singola procedura.

L'archiviazione delle segnalazioni presentate mediante la piattaforma informatica, nonché della documentazione allegata o sviluppata nel corso dell'attività di gestione delle medesime, viene effettuata utilizzando la piattaforma informatica. La documentazione in originale, cartacea e/o elettronica, viene conservata per il tempo necessario alla gestione della specifica segnalazione e, comunque, non oltre i cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

4.2 Finalità del trattamento

Le finalità delle operazioni di trattamento consistono nell'acquisizione, nell'istruzione e nella gestione delle segnalazioni. In particolare, i dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite delle quali sia venuto a conoscenza in ragione del proprio rapporto di servizio con l'Ente commesse dai soggetti che a vario titolo interagiscono con il medesimo, vengono trattati allo scopo di effettuare le necessarie attività preliminari ed istruttorie (inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati) volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

4.3 Base giuridica del trattamento

I dati personali sono trattati dal Comune, in qualità di titolare del trattamento, nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, con particolare riferimento al compito di accertare eventuali illeciti denunciati nell'interesse dell'integrità dell'Ente. Le operazioni di

trattamento sono altresì svolte perché necessarie per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, ai sensi degli artt. 6, comma 1, let. c), 9, comma 2, let. b) e 10 GDPR e 4, comma 1, del Decreto Whistleblowing.

4.4 Categorie di interessati

Le persone fisiche cui i dati personali trattati si riferiscono sono: (*i*) i soggetti che effettuano una segnalazione; (*ii*) i soggetti nei confronti dei quali viene effettuata una segnalazione; (*iii*) i soggetti indicati o individuati quali possibili testimoni o beneficiari di protezione contro le ritorsioni.

4.5 Categorie di dati trattati

I dati trattati consistono in: (*i*) dati anagrafici (nome e cognome), nel caso in cui il segnalante decida di comunicare la propria identità; (*ii*) *key code* generato dalla piattaforma informatica di segnalazione; (*iii*) informazioni relative alla categoria/qualifica ricoperta e/o ai rapporti lavorativi, professionali e/o commerciali, intrattenuti con il titolare del trattamento; (*iv*) dati e informazioni relative alla violazione denunciata, anche riferite a soggetti terzi, che il segnalante decide di comunicare per meglio circostanziare la propria segnalazione; (*v*) eventuali categorie particolari di dati personali e/o dati giudiziari, se contenuti nei campi a testo libero presenti nel modulo di segnalazione o altrimenti appresi nel corso dell'attività istruttoria.

4.6 Categorie di destinatari dei dati personali

I dati personali raccolti sono trattati dal personale dell'Ente, che agisce sulla base di specifiche istruzioni fornite in ordine a finalità e modalità del trattamento; da Whistleblowing Solutions Impresa Sociale S.r.l. quale fornitore del servizio di erogazione e gestione operativa della piattaforma tecnologica di digital whistleblowing in qualità di Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679; da Seeweb S.r.l. e Transparency International Italia, rispettivamente quali subfornitori del servizio di hosting dei sistemi informatici e del servizio di supporto utenti e amministratore di sistema. I dati personali oggetto di trattamento possono inoltre essere comunicati, se del caso: all'Autorità Giudiziaria, all'Autorità Nazionale Anti Corruzione (ANAC), alla Corte dei Conti.

4.7 Ruoli e responsabilità del trattamento

Titolare del trattamento è il Comune di Spoleto (C.F. 00316820547), con sede in Piazza del Comune, n. 1 – 06049 Spoleto (PG).
Responsabile del trattamento è: (i) Whistleblowing Solutions Impresa Sociale S.r.l. (C.F. e P.I. 09495830961), con sede in Viale Abruzzi, n. 13/A – 20129 Milano (MI), fornitore dell'applicativo "GlobaLeaks" impiegato per l'acquisizione e la gestione delle segnalazioni di condotte illecite.
Sub-responsabili del trattamento, designati da Whistleblowing Solutions Impresa Sociale S.r.l., sono: (i) Seeweb S.r.l. (C.F. e P.I. 02043220603), con sede in Via Armando Vona, n. 66 – 03100 Frosinone (FR), fornitore dei servizi di gestione dell'infrastruttura IaaS (hosting dei sistemi informatici); (ii) Transparency International Italia (C.F. 97186250151), con sede in Piazzale Carlo Maciachini, n. 11 – 20159 Milano (MI), fornitore del servizio di supporto utenti e amministratore di sistema.

4.8 Trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo e organizzazioni internazionali

Tutti i dati oggetto di trattamento sono elaborati all'interno dell'Unione Europea e non ne è previsto il trasferimento verso Paesi non appartenenti allo Spazio Economico Europeo o organizzazioni internazionali.

4.9 Fonte dei dati

I dati sono: (i) raccolti direttamente presso l'interessato, per quanto concerne il segnalante; (ii) acquisiti presso terzi, sia mediante la segnalazione iniziale che nell'ambito dell'attività istruttoria, per quanto concerne il segnalante, i soggetti nei confronti dei quali viene effettuata una segnalazione, i soggetti indicati o individuati quali possibili testimoni o beneficiari di protezione contro le ritorsioni.

4.10 Risorse di supporto al trattamento

4.10.1 Risorse tecniche

Le operazioni di acquisizione e gestione delle segnalazioni vengono effettuate principalmente impiegando una piattaforma informatica basata sul software "GlobaLeaks", sviluppato e fornito da Whistleblowing Solutions Impresa Sociale S.r.l.
La piattaforma informatica è dotata di un protocollo di crittografia che garantisce la segregazione dell'identità del segnalante dal contenuto della segnalazione.
L'architettura di sistema è costituita principalmente da: *(i)* un cluster di due firewall perimetrali; *(ii)* un cluster di due server fisici dedicati; *(iii)* una Storage Area Network pienamente ridondata.
L'architettura di rete prevede: *(i)* un firewall perimetrale e segregazione della rete in molteplici VLAN, al fine di isolare le differenti componenti secondo la loro differente natura in modo da limitare ogni esposizione in caso di vulnerabilità su una singola componente; *(ii)* una VPN, per consentire l'accesso alla gestione dell'infrastruttura ad un limitato e definito insieme di amministratori di sistema; *(iii)* l'implementazione del protocollo di cifratura TLS 1.2+ su ogni connessione di rete; *(iv)* la limitazione all'effettiva necessità dell'esposizione di rete di ogni macchina virtuale istanziata; *(v)* la configurazione di tutti i dispositivi ed i processi applicativi in modo da non registrare alcun tipo di log delle azioni compiute dal segnalante o altre informazioni che potrebbero consentirne l'identificazione, quali indirizzi IP e User Agents; *(vi)* l'abilitazione alla navigazione dell'applicativo tramite Tor Browser, per finalità di accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.
La piattaforma informatica di segnalazione è basata sul software libero ed open-source "GlobaLeaks", erogato in modalità S.a.a.S. (software-as-a-service).
Confezionato per Linux Debian e Ubuntu LTS (Long Term Support), presenta un backend sviluppato con piena compatibilità python 3.x e un frontend in Javascript basato su AngularJS .
Per motivi di sicurezza, è autonomo in tutti i componenti infrastrutturali, come il server Web incorporato che sfrutta il framework di rete ad alte prestazioni Twisted insieme alla generazione automatica di certificato digitale gratuito utilizzando Let'sEncrypt e Anonymous Onion Services utilizzando Tor. Esegue operazioni di crittografia con GnuPG e crittografia libreria basata su OpenSSL
Per ogni invio, l'applicazione fornisce al Whistleblower una ricevuta che può utilizzare per verificare lo stato dell'invio, scambiare messaggi con i destinatari e fornire materiale aggiuntivo. Ai destinatari vengono inviate notifiche crittografate OpenPGP su novità o aggiornamenti sulle comunicazioni degli informatori.

In aggiunta a GlobaLeaks, utilizzato in via principale per l'implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto, vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile.
Vengono anche in modo limitato utilizzate alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale.
Le tecnologie impiegate sono: (i) Debian/Linux (principale sistema operativo utilizzato); (ii) Postfix (mail server); (iii) Bind9 (dns server); (iv) OPNSense (firewall); (v) OpenVPN (vpn); (vi) VMware (virtualizzazione delle macchine); (vii) Veeam (backup); (viii) Plesk (realizzazione siti web di facciata del progetto).
I server eseguono software VMware e vCenter abilitando funzionalità di High Availability; su VMware vengono istanziate macchine virtuali Debian/Linux nelle sole version Long Term Support (LTS). Ogni macchina virtuale Debian implementa configurazione securizzata con: Full Disk Encryption (lvm/crypto), SecureBoot, Apparmor, Iptables;
Entrambi i server fisici eseguono una macchina virtuale di Key Management System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici componenti il cluster.

4.10.2 Risorse organizzative

L'attività di gestione delle segnalazioni è regolata dalla Procedura per la gestione delle segnalazioni trasmesse al Comune di Spoleto, la quale stabilisce , tra l'altro: (*i*) gli specifici *steps* procedurali da intraprendere per la gestione del ciclo di vita della segnalazione, inclusi gli accorgimenti da intraprendere qualora si ponga l'esigenza di rivelare l'identità del segnalante; (*ii*) il divieto di ritorsioni nei confronti dell'autore della segnalazione e delle persone beneficiarie della protezione; (*iii*) l'obbligo di non acquisire o comunque cancellare ogni dato manifestamente superfluo o non utile alla trattazione della segnalazione; (*iv*) la sottrazione della segnalazione dalla disciplina dell'accesso agli atti di cui agli artt. 22 e ss. della Legge n. 241/1990.

4.10.3 Risorse umane

L'attività è curata dal RPCT in qualità di Gestore delle segnalazioni.

5. Valutazioni

5.1. Rispetto dei principi fondamentali del trattamento

5.1.1. Liceità, trasparenza e correttezza

Il trattamento è: (*i*) **lecito** perché svolto conformemente alle prescrizioni di cui al D. Lgs. n. 24 del 10 marzo 2023; (*ii*) **trasparente** perché gli interessati sono adeguatamente ed esaustivamente informati di tutti gli aspetti rilevanti *ex* artt. 13 e 14 GDPR prima che il trattamento abbia inizio; (*iii*) **corretto** perché limitato a quanto previsto dalla legge e dichiarato agli interessati, senza che questi vengano tratti in inganno o fuorviati sulle reali finalità e modalità di trattamento o che vengano effettuate operazioni non previste.

Valutazione: Accettabile

5.1.2. Necessità e proporzionalità del trattamento

Le operazioni di trattamento sono: (*i*) necessarie poiché imposte da norme di legge; (ii) proporzionate poiché limitate a quanto previsto dalla legge.

Valutazione: Accettabile

5.1.3. Limitazione della finalità

Le finalità perseguite mediante le operazioni di trattamento sono: (*i*) determinate poiché delineate con sufficiente precisione; (*ii*) esplicite poiché chiaramente indicate agli interessati nelle informative; e (*iii*) legittime poiché espressamente previste da norme di legge.
Non è previsto alcun successivo trattamento dei medesimi dati.

Valutazione: Accettabile

5.1.4. Limitazione della conservazione

La documentazione in originale, cartacea e/o elettronica, viene conservata per il tempo necessario al trattamento della specifica segnalazione e, comunque, non oltre i cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Valutazione: Accettabile

5.1.5. Esattezza dei dati

Stanti la natura e le finalità del trattamento, l'esattezza dei dati contenuti nella segnalazione è rimessa al segnalante, il quale può modificare in ogni momento la segnalazione presentata, anche integrandola con ulteriori elementi (se del caso, con le proprie informazioni anagrafiche). La verifica della fondatezza dei dati personali comunicati dal segnalante costituisce l'oggetto della fase istruttoria.

Valutazione: Accettabile

5.1.6. Minimizzazione dei dati

In linea generale, i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.
I dati particolari e giudiziari volontariamente comunicati dal segnalante, saranno utilizzati solo ove strettamente necessari per la gestione della segnalazione, nel pieno rispetto dei principi di proporzionalità e necessità e, se ritenuti irrilevanti ai fini della stessa, non saranno oggetto di ulteriore trattamento.

Valutazione: Accettabile

5.1.7. Rapporti con i terzi

I rapporti con il fornitore Whistleblowing Solutions Impresa Sociale S.r.l. sono regolati mediante apposito accordo di "nomina a responsabile del trattamento", che rispetta tutti i requisiti di forma e di contenuto previsti dagli artt. 28 e 29 GDPR.
Whistleblowing Solutions Impresa Sociale S.r.l. ha regolato i rapporti con i sub-responsabili del trattamento mediante appositi accordi di "nomina a sub-responsabile del trattamento", che rispettano i requisiti di forma e contenuto previsti dall'art. 28, comma 4 GDPR.

Valutazione: Accettabile

5.1.8. Diritti degli interessati

Il diritto degli interessati all'informazione è assicurato mediante la somministrazione di apposita informativa, rispondenti ai requisiti di contenuto previsti dagli artt. 13 e 14 GDPR.
L'informativa è: (i) per coloro che decidono di impiegare il canale informatico, somministrata in occasione

dell'accesso alla piattaforma informatica, la quale è tecnicamente configurata in modo da richiedere l'attestazione di previa visione e comprensione prima di consentire l'accesso al modulo da compilare per effettuare la segnalazione; (ii) per coloro che decidono di ricorrere ad altra modalità di segnalazione, resa disponibile sul sito *web* del Comune, nella sezione informativa dedicata al whistleblowing.
Gli interessati possono esercitare i propri diritti – nei limiti stabiliti dall'art. 2-*undecies* del Codice Privacy – rivolgendosi al Titolare presso i recapiti indicati nell'informativa.

Valutazione: accettabile

5.1.9. Sicurezza del trattamento

La piattaforma informatica impiegata per l'acquisizione, la gestione e la conservazione delle segnalazioni è protetta mediante le seguenti misure tecniche ed organizzative di sicurezza:
(i) **crittografia**: l'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington. Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. Il protocollo crittografico impiegato è descritto al link https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html;
(ii) **controllo degli accessi logici**: l'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password;
(iii) **tracciabilità**: l'applicativo GlobaLeaks implementa 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. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent;
(iv) **archiviazione**: l'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. 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;
(v) **gestione delle vulnerabilità tecniche**: 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. A questi si aggiunge la peer review indipendente realizzata dalla comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente;
(vi) **back-up**: I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery;
(vii)**manutenzione:** è 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 Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti;
(viii) **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;
(ix) **sicurezza dell'hardware:** 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, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24. I datacenter del fornitore IaaS sono certificati ISO27001;
(x) **gestire gli incidenti di sicurezza e le violazioni dei dati personali:** Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.
(xi) **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;
(xii)**audit**: la piattaforma è sottoposta a periodici audit di sicurezza, incluse attività di *penetration test*.
La piattaforma informatica ha ricevuto le seguenti certificazioni: (i) ISO 27001 ("Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks"); (ii) ISO27017 ("controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud"); (iii) ISO27018 per la protezione dei dati personali nei servizi Public Cloud; (iv) Qualifica AGID; (v) Certificazione CSA Star.
I sistemi informatici aziendali e gli apparati di sicurezza informatica sono configurati in modo da non tracciare il traffico web, proveniente da connessioni aziendali o da dispositivi attestati su connessioni aziendali, verso la piattaforma informatica impiegata per l'acquisizione e la gestione delle segnalazioni.

Il Gestore ha ricevuto specifiche istruzioni comportamentali.

L'accesso effettuato alla piattaforma informatica e le operazioni compiute da ciascun profilo sono registrate mediante *log files*.

Valutazione: Accettabile

5.2. Rischi
I principali rischi derivanti dalle operazioni di trattamento di dati personali effettuati consistono in: (i) **ritorsioni** e/o **pregiudizi reputazionali** a detrimento del segnalante, delle persone beneficiarie della protezione e/o della persona nei confronti della quale la segnalazione è elevata; (ii) condotte aziendali dirette ad impedire che il segnalante usufruisca delle tutele prescritte dalla normativa; (iii) violazione del diritto di difesa del segnalato in seno al procedimento disciplinare.
5.2.1. Ritorsioni e/o pregiudizi reputazionali
I **fattori di rischio** individuati in relazione al rischio di ritorsioni consistono in:
(i) **divulgazione non autorizzata dell'identità del segnalante**.
Il rischio di ritorsioni e/o di pregiudizi reputazionali è ipotizzabile nel caso in cui l'identità del segnalante sia rilevata all'interno dell'ente al di fuori dei casi previsti dalla legge.
Le vulnerabilità possono essere individuate: (i) nell'assenza di adeguata formazione da parte del/i soggetti incaricati di acquisire e gestire le segnalazioni; (ii) nell'assenza di istruzioni chiare in relazione alle corrette

modalità di trattamento dei dati personali contenuti nella segnalazione; (iii) nell'assenza di regolamentazione della gestione delle violazioni di dati personali e/o dei relativi processi di notifica.
L'**impatto inerente** derivante dal verificarsi del fattore di rischio è **elevato**, perché gli interessati potrebbero essere vittime o comunque esposti a comportamenti lesivi dei propri diritti fondamentali, con particolare riguardo a quei diritti che trovano esplicazione nel contesto dei rapporti lavorativi e a quei diritti che possono trovare realizzazione soltanto mediante l'azione dell'ente pubblico locale.

La **probabilità astratta** del verificarsi del **fattore di rischio**, in assenza di misure tecniche ed organizzative di mitigazione, è **media**.

(ii) <u>accesso non autorizzato ai dati relativi all'identità del segnalante o alla segnalazione.</u>
Il rischio di ritorsioni e/o di pregiudizi reputazionali è ipotizzabile nel caso in cui l'identità del segnalante, delle persone beneficiarie della protezione e/o della persona nei confronti della quale la segnalazione è elevata, o la segnalazione medesima, siano conosciuti da soggetti non autorizzati ad accedere a tali informazioni.
Le vulnerabilità possono essere individuate, quanto alle segnalazioni effettuate mediante piattaforma informatica: (*i*) nell'assenza di protocolli crittografici; (*ii*) nell'assenza o nel mancato aggiornamento di adeguati strumenti di protezione del *software* e delle banche dati impiegate per la gestione delle segnalazioni contro l'azione di virus informatici, malware ed altre tipologie di attacchi informatici; (*iii*) nell'assenza di profilazione degli utenti abilitati ad accedere al back-end della piattaforma informatica per la gestione delle segnalazioni; (*iv*) nell'assenza di e/o nell'insufficiente robustezza dei meccanismi di autenticazione impiegati per l'accesso al back-end della piattaforma informatica per la gestione delle segnalazioni; (*v*) nell'assenza di misure di protezione fisica dei locali che ospitano le componenti *hardware* dell'infrastruttura informatica.
Le vulnerabilità possono essere individuate, quanto alle segnalazioni effettuate mediante altra modalità: (*i*) nell'assenza di adeguata formazione da parte degli addetti al protocollo; (*ii*) nell'assenza di adeguate misure di custodia dei plichi cartacei o degli appunti presi dal Gestore nell'ambito dell'audizione orale.
L'**impatto inerente** derivante dal verificarsi del fattore di rischio è **elevato**, perché gli interessati potrebbero essere vittime o comunque esposti a comportamenti lesivi dei propri diritti fondamentali, con particolare riguardo a quei diritti che trovano esplicazione nel contesto dei rapporti lavorativi e a quei diritti che possono trovare realizzazione soltanto mediante l'azione dell'ente pubblico locale.

La **probabilità astratta** del verificarsi del **fattore di rischio**, in assenza di misure tecniche ed organizzative di mitigazione, è **media**.

(iii) <u>modifica non autorizzata dei dati relativi all'identità del segnalante o alla segnalazione.</u>
Il rischio di ritorsioni e/o di pregiudizi reputazionali è ipotizzabile nel caso in cui i dati relativi all'identità del segnalante o alla segnalazione vengano modificati abusivamente, alterandoli per farla risultare attribuibile ad un soggetto diverso da quello da cui realmente proviene o per farne risultare irricevibile o calunnioso il contenuto.

Le vulnerabilità possono essere individuate: (*i*) nell'assenza di strumenti di tracciamento delle operazioni effettuate da parte dell'amministratore di sistema, del Gestore e dei delegati da questi autorizzati al trattamento; (*ii*) nell'assenza di copie di *back-up* dei dati.

L'**impatto inerente** derivante dal verificarsi del fattore di rischio è **elevato**, perché gli interessati potrebbero essere vedersi preclusa la possibilità di segnalare violazioni o accusati ingiustamente di aver presentato

segnalazioni infondate o calunniose, con possibili riflessi pregiudizievoli sul piano lavorativo e/o personale.

La **probabilità astratta** del verificarsi del **fattore di rischio**, in assenza di misure tecniche ed organizzative di mitigazione, è **bassa**.

(iv) **identificazione indiretta del segnalante**.

Il rischio di ritorsioni e/o di pregiudizi reputazionali è ipotizzabile nel caso in cui il segnalante, che abbia scelto o meno di rimanere anonimo, risulti comunque identificabile a prescindere da un'azione intenzionale in tal senso o di un errore da parte degli operatori coinvolti.

La vulnerabilità può essere individuata in una eventuale errata configurazione dei sistemi informatici interni all'ente, per effetto della quale è possibile tracciare il traffico web effettuato a partire dalle connessioni locali verso la piattaforma informatica impiegata per l'acquisizione e la gestione delle segnalazioni o le chiamate effettuate.
La causa della minaccia potrebbe, altresì, essere riconducibile ad un errore imputabile ai soggetti autorizzati al trattamento dei dati inerenti la segnalazione (ad esempio nel caso in cui, nel corso dell'istruttoria, in sede di interlocuzione o scambio di documentazione con il RPCT o autorizzati, vengano fornite informazioni di dettaglio che indirettamente ma univocamente consentano l'identificazione del segnalante).

L'**impatto inerente** derivante dal verificarsi del fattore di rischio è **elevato**, perché gli interessati potrebbero essere vittime o comunque esposti a comportamenti lesivi dei propri diritti fondamentali, con particolare riguardo a quei diritti che trovano esplicazione nel contesto dei rapporti lavorativi e a quei diritti che possono trovare realizzazione soltanto mediante l'azione dell'ente pubblico locale.

La **probabilità astratta** del verificarsi del **fattore di rischio**, in assenza di misure tecniche ed organizzative di mitigazione, è **media**.

(v) **rivelazione dell'identità del segnalante, autorizzata da quest'ultimo**.

Il rischio di ritorsioni e/o di pregiudizi reputazionali è ipotizzabile anche nel caso in cui l'identità del segnalante sia rivelata conformemente alle volontà di quest'ultimo, il quale abbia prestato il proprio consenso alla relativa divulgazione.

L'**impatto inerente** derivante dal verificarsi del rischio è **elevato**, perché gli interessati potrebbero essere vittime o comunque esposti a comportamenti lesivi dei propri diritti fondamentali, con particolare riguardo a quei diritti che trovano esplicazione nel contesto dei rapporti lavorativi e a quei diritti che possono trovare realizzazione soltanto mediante l'azione dell'ente pubblico locale.

La **probabilità astratta** del verificarsi del **fattore di rischio**, in assenza di misure tecniche ed organizzative di mitigazione, è **media**.

5.2.2. Rischi connessi all'impossibilità, per il segnalante, di usufruire delle tutele di cui al D.Lgs

24/2023

I **fattori di rischio** individuati in relazione al rischio in esame consistono in:

(i) **indisponibilità dei dati relativi all'avvenuta presentazione di una segnalazione, anche in forma anonima**.

Il rischio in esame è ipotizzabile nel caso in cui il segnalante, che sia stato destinatario di un provvedimento datoriale ritorsivo, non abbia modo di dimostrare di aver presentato una segnalazione e di essere, pertanto, beneficiario della protezione prevista dalla legge, a causa della perdita o della cancellazione, accidentali o abusive, dei dati relativi alla medesima.

Le vulnerabilità possono essere individuate nell'assenza di copie di *back-up* dei dati.

L'**impatto inerente** derivante dal verificarsi del fattore di rischio è **elevato**, perché gli interessati potrebbero trovarsi sprovvisti, in concreto, delle possibilità di beneficiare delle tutele offerte dalla legge.

La **probabilità astratta** del verificarsi del **fattore di rischio**, in assenza di misure tecniche ed organizzative di mitigazione, è **bassa**.

5.2.3. Rischi connessi all'impossibilità, per il segnalato, di esercitare le proprie difese in seno al procedimento disciplinare

I **fattori di rischio** individuati in relazione al rischio in esame consistono in:

(i) **violazione dei diritti riconosciuti dagli artt. 15 – 22 GDPR**.

Il rischio in esame è ipotizzabile nel caso in cui il segnalato, nell'ambito di un procedimento disciplinare instaurato nei suoi confronti, non sia posto in condizioni di conoscere l'identità del segnalante ancorchè ciò sia indispensabile per l'esercizio del suo diritto di difesa; oppure nel caso contrario in cui il segnalato, all'atto di esercitare il proprio diritto di accesso nel contesto di un procedimento disciplinare basato, oltre che sulla segnalazione, su ulteriori elementi probatori acquisiti in fase istruttoria, si veda rivelato indebitamente il nominativo del segnalante.

Le vulnerabilità possono essere individuate: (*i*) nell'assenza di chiare indicazioni circa la necessità di provvedere alla somministrazione delle informazioni previste ex artt. 13 e 14 GPDR una volta venuto meno l'obbligo di segretezza; (*ii*) nell'assenza di adeguata formazione da parte del soggetto incaricato di acquisire e gestire le segnalazioni e/o le richieste di esercizio dei diritti riconosciuti dagli artt. 15 – 22 GDPR.

L'**impatto inerente** derivante dal verificarsi del fattore di rischio è **elevato**, perché gli interessati, in assenza di informativa da parte del titolare del trattamento circa l'avvenuta presentazione di una segnalazione nei loro confronti e le facoltà loro attribuite dagli artt. 15-22 del GDPR, potrebbero ignorare la possibilità di esercitare i diritti riconosciuti dalla legge (a partire dal diritto di accesso) o vedersi negato in concreto il relativo esercizio anche al di fuori dei presupposti stabiliti dal Codice Privacy e/o dal Decreto Whistleblowing; oppure giungere a conoscenza, al di fuori dei presupposti di legge, dell'identità del segnalante.

La **probabilità astratta** del verificarsi del **fattore di rischio**, in assenza di misure tecniche ed organizzative di mitigazione, è **elevata**.

5.3. Misure tecniche ed organizzative

5.3.1. Con riferimento al rischio di ritorsioni e/o di pregiudizi reputazionali ed ai **relativi fattori di rischio, le misure utili a ridurre la probabilità e**/o l'impatto, intervenendo sulle singole vulnerabilità, sono:

- in relazione alla divulgazione non autorizzata dell'identità del segnalante: (a) la formazione dei soggetti autorizzati al trattamento; (b) la previsione di istruzioni comportamentali vincolanti relative al trattamento dei dati personali.

Valutazione: accettabile

- in relazione all'accesso non autorizzato ai dati relativi all'identità del segnalante, delle persone beneficiarie della protezione e/o delle persone nei cui confronti la segnalazione è elevata: (a) l'impiego di protocolli di cifratura del canale di segnalazione informatico, sia di tipo "*at-rest*" che "*in transit*"; (b) l'implementazione e l'aggiornamento costante di firewall, antivirus e soluzioni antimalware; (c) l'attribuzione di profili autorizzati ad accedere al *back-end* della piattaforma informatica di segnalazione ai soli soggetti autorizzati; (d) l'implementazione di meccanismi di autenticazione di tipo MFA; (e) la formazione del personale preposto al protocollo in merito al divieto di apertura delle buste ricevute; (f) la conservazione sicura dei plichi cartacei e degli appunti presi da parte del Gestore e degli addetti al protocollo.

Valutazione: accettabile

- in relazione alla modifica non autorizzata dei dati relativi all'identità del segnalante o alla segnalazione: (a) l'impiego di strumenti di tracciamento delle operazioni compiute dall'amministratore di sistema e dai soggetti autorizzati, mediante generazione e conservazione di *log files* aventi caratteristiche di completezza ed inalterabilità; (b) l'effettuazione periodica di copie di *back-up* dei dati relativi alla segnalazione.

Valutazione: accettabile

- in relazione all'identificazione indiretta del segnalante: (a) configurazione dei sistemi informatici interni all'ente e degli applicativi di sicurezza (ad es. di tipo firewall) in modo da non tracciare il traffico web, attestato su connessioni locali, verso la piattaforma informatica impiegata per l'acquisizione e la gestione delle segnalazioni; (b) la formazione dei soggetti autorizzati al trattamento

Valutazione: accettabile

- in relazione alla rivelazione dell'identità del segnalante, autorizzata da quest'ultimo: (a) previsione, all'interno della_Procedura per la gestione delle segnalazioni trasmesse al Comune di Spoleto, del divieto di ritorsioni nei confronti del segnalante.

Valutazione: accettabile

5.3.2. Con riferimento al rischio di impossibilità, per il segnalante, di esercitare il proprio diritto alla protezione contro le ritorsioni, le misure utili a ridurre la probabilità e/o l'impatto, intervenendo sulle singole vulnerabilità, sono:

- in relazione alla indisponibilità dei dati relativi all'avvenuta presentazione di una segnalazione, anche in forma anonima: (a) l'effettuazione periodica di copie di *back-up* dei dati relativi alla segnalazione, a

disposizione del solo Gestore.

Valutazione: accettabile

5.3.3. Con riferimento al rischio di impossibilità, per il segnalato, di far valere il proprio diritto di difesa in seno al procedimento disciplinare, le misure utili a ridurre la probabilità e/o l'impatto, intervenendo sulle singole vulnerabilità, sono:

- in relazione al diniego dei diritti riconosciuti dagli artt. 15 – 22 GDPR: (a) la previsione, all'interno della Procedura per la gestione delle segnalazioni trasmesse al Comune di Spoleto, in caso di avvio di un procedimento disciplinare a carico del segnalato, dell'obbligo di comunicare tempestivamente, e quanto prima possibile, a quest'ultimo, le informazioni che possono essere rivelate, previste dall'art. 14 GDPR ed i diritti attribuiti dal GDPR; (b) la formazione dei soggetti autorizzati al trattamento.

Valutazione: accettabile

SEZIONE III

6. Coinvolgimento degli interessati o dei relativi rappresentanti

L'implementazione di un canale di segnalazione interno è stata resa nota alle OO.SS..

7. Presupposti per la consultazione preventiva ex art. 36 GDPR

Non si ravvisano i presupposti per la consultazione preventiva.

Il presente documento è redatto e firmato in formato digitale ai sensi del decreto legislativo 7 marzo 2005, n° 82 recante il "Codice dell'amministrazione digitale"

Il Segretario Generale
Dott. **Mario Ruggieri**

Il Responsabile del Servizio Sistemi Informativi
dott. Paolo Scarabottini

Parere favorevole del DPO
Avv. Francesca Potì