COMUNE DI FOLIGNO

Provincia di Perugia

Seduta del 31-01-2023

Deliberazione della Giunta Comunale

n. 40 del 31-01-2023

OGGETTO: ART. 54BIS DEL D.LGS. 165/2001 - PROCEDIMENTO PER LE SEGNALAZIONI DI ILLECITI DA PARTE DI DIPENDENTI O COLLABORATORI DELL'ENTE - APPROVAZIONE DPIA (VALUTAZIONE DI IMPATTO) AI FINI DELLA NORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI DI CUI AL REG.UE 2016/679

L'anno duemilaventitre il giorno trentuno del mese di Gennaio alle ore 10:35, nella apposita sala, si è riunita la Giunta Comunale, convocata ai sensi del Regolamento per il funzionamento della Giunta Comunale e alla quale risultano:

N	Cognome e Nome	Carica	Presenze
1	ZUCCARINI STEFANO	SINDACO	Presente
2	BARILI DECIO	ASSESSORE	Presente
3	CESARO MARCO	ASSESSORE	Presente
4	CETORELLI AGOSTINO	ASSESSORE	**Assente**
5	DE BONIS PAOLA	ASSESSORE	**Assente**
6	GIULIANI MICHELA	ASSESSORE	Presente
7	MELONI RICCARDO	VICE SINDACO	Presente
8	UGOLINELLI ELISABETTA	ASSESSORE	Presente

PRESENTI: 6 - ASSENTI: 2

Partecipa il SEGRETARIO GENERALE DOTT. PAOLO RICCIARELLI.

Constatato il numero legale degli intervenuti, assume la presidenza il SINDACO AVV. STEFANO ZUCCARINI ed invita la Giunta all’esame dell’oggetto su riferito.

LA GIUNTA COMUNALE

VISTA l'allegata proposta redatta in data 30-01-2023 dal SEGRETARIO GENERALE, che qui si intende integralmente trascritta;

RITENUTO di condividere il documento per le motivazioni ivi contenute e pertanto di far propria la proposta presentata;

VISTO che la stessa riporta il parere favorevole di regolarità tecnica previsto dall'Art.49 comma 1 del D.Lgs. 267/2000;

DATO ATTO che la proposta della presente deliberazione è stata esaminata dall'Area Servizi Finanziari, ai sensi dell'art. 49, comma 1, del D.lgs. 267/2000, e che la stessa l'ha ritenuta priva di rilevanza contabile;

Con voti unanimi e favorevoli, validamente espressi nei modi e forme di legge;

DELIBERA

1. Di approvare, per le motivazioni di cui in premessa, la Valutazione di impatto (DPIA) – Revisione 28/01/2023 - di cui all'art. 35 del Reg.UE 2016/679 relativa al trattamento dati attuato mediante la Piattaforma telematica gratuita di Trasparency International Italia tramite Whistleblowing Solutions Impresa Sociale S.r.l., che gestisce le segnalazioni da parte dei dipendenti e dei collaboratori del Comune di Foligno di reati o irregolarità di cui siano venuti a conoscenza in ragione del rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing), che come parte integrante e sostanziale si allega al presente atto.

2. Di dare atto che sul documento è stato acquisito il parere favorevole del referente del Responsabile Protezione dati - DPO - Avv. Annalisa Luciani che ha attestato l'assenza di rischi elevati rispetto al trattamento in parola.

3. Di dare atto che la Valutazione di Impatto - DPIA verrà pubblicata sul sito del Comune di Foligno, sezione Amministrazione Trasparente – Altri contenuti – Prevenzione della Corruzione – Whistleblowing.

INFINE, con separata ed unanime votazione validamente espressa nelle forme di legge, DELIBERA di dichiarare il presente atto immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D.Lgs. 267/2000.

^^^^^

SEGRETARIO GENERALE

AREA SEGRETERIA GENERALE

Proposta di Atto di Giunta

Alla Giunta

RICHIAMATE:

- la deliberazione n. 12 del 29/03/2022, immediatamente eseguibile, con cui il Consiglio Comunale ha approvato il Documento Unico di Programmazione (DUP) 2022-2024 – nota di aggiornamento;

- la deliberazione n. 13 del 29/03/2022, immediatamente eseguibile, con cui il Consiglio Comunale ha approvato il bilancio di previsione esercizio 2022-2024;

- la deliberazione n. 271 del 15/06/2022, immediatamente eseguibile, con la quale la Giunta Comunale ha approvato il Piano Esecutivo di Gestione (P.E.G.), il Piano degli Obiettivi (P.D.O.) e il Piano della Performance (P.P.) anno 2022 e pluriennale 2022-2024";

VISTI:

- il Decreto del Ministero dell'Interno 13/12/2022, pubblicato nella G.U. n. 295 del 19/12/2022, con cui è stato disposto il differimento al 31 marzo 2023 del termine per la deliberazione del Bilancio di previsione 2023/2025 degli enti locali;

- la Legge 29/12/2022, n. 197, recante il "Bilancio di previsione dello Stato per l'anno finanziario 2023 e Bilancio pluriennale per il triennio 2023–2025", pubblicata nella G.U. n. 303 – supplemento ordinario n. 43 del 29/12/2022, che all'articolo 1, comma 775, prevede che "*In via eccezionale e limitatamente all'anno 2023, in considerazione del protrarsi degli effetti economici negativi della crisi ucraina, gli enti locali possono approvare il Bilancio di previsione con l'applicazione della quota libera dell'avanzo, accertato con previsione del rendiconto 2022. A tal fine il termine per l'approvazione del Bilancio di previsione per il 2023 è differito al 30 aprile 2023";*

PRESO ATTO che, a seguito di tale differimento, il Comune si trova automaticamente in esercizio provvisorio;

RICORDATO CHE:

- il Comune di Foligno, dal 29/11/2019, si è dotato della piattaforma gratuita di Traparency International Italia mediante Whistleblowing Solutions Impresa Sociale S.r.l. per gestire il sistema delle segnalazioni da parte di dipendenti e collaboratori dell'Ente (c.d. whistleblowing) di reati o irregolarità di cui siano venuti a conoscenza in ragione del rapporto di lavoro, ai sensi dell'art. 54bis del D.Lgs. 165/2001;

- la piattaforma consente di gestire le eventuali segnalazioni in maniera riservata, al fine di evitare, come prevede la norma, che l'identità del segnalante venga rivelata e, di conseguenza, che lo stesso possa subire qualsiasi conseguenza negativa sul posto di lavoro per effetto della segnalazione;

- l'Autorità Nazionale Anticorruzione (ANAC), con apposita deliberazione n. 469 del 09.6.2021 ha approvato specifiche 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)";

DATO ATTO CHE:

- Il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (c.d. GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati è applicabile dal 25 maggio 2018 ed è stato attuato in Italia per mezzo del D.Lgs. 101/2018 mediante l'aggiornamento del T.U. sulla Privacy, D.Lgs 196/2003;

- L'art. 35 del GDPR prevede 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, può presentare un rischio elevato 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. Una singola valutazione (definita valutazione di impatto o DPIA) può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi". Inoltre, al paragrafo 7 il legislatore europeo stabilisce: "la valutazione contiene 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;

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;

DATO ATTO che la Valutazione di impatto in discorso è stata predisposta con il supporto del Segretario Generale, in qualità di Responsabile della prevenzione della corruzione e della trasparenza (RPCT) e del Responsabile del Servizio Sistemi Informativi;

PRECISATO CHE La DPIA costituisce allegato al Registro dei trattamenti tenuto dal Comune di Foligno – approvato con deliberazione di Giunta Comunale n. 305 del 7/6/2019 e successive modifiche ed integrazioni - e verrà pubblicata sul sito del Comune di Foligno, sezione Amministrazione Trasparente – Altri contenuti – Prevenzione della Corruzione – Whistleblowing;

DATO ATTO CHE sul documento è stato acquisito il parere favorevole del referente del Responsabile Protezione dati - DPO - Avv. Annalisa Luciani che ha attestato l'assenza di rischi elevati rispetto al trattamento in parola;

VISTA l'allegata Valutazione di Impatto (DPIA) – Revisione 28/01/2023 - che si compone del documento e di n. 5 allegati;

RITENUTO quindi di procedere all'approvazione della Valutazione di Impatto (DPIA);

si propone quanto segue:

1. Di approvare, per le motivazioni di cui in premessa, la Valutazione di impatto (DPIA) – Revisione 28/01/2023 - di cui all'art. 35 del Reg.UE 2016/679 relativa al trattamento dati attuato mediante la Piattaforma telematica gratuita di Trasparency International Italia tramite Whistleblowing Solutions Impresa Sociale S.r.l., che gestisce le segnalazioni da parte dei dipendenti e dei collaboratori del Comune di Foligno di reati o irregolarità di cui siano venuti a conoscenza in ragione del rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing), che come parte integrante e

sostanziale si allega al presente atto.

2. Di dare atto che sul documento è stato acquisito il parere favorevole del referente del Responsabile Protezione dati - DPO - Avv. Annalisa Luciani che ha attestato l'assenza di rischi elevati rispetto al trattamento in parola.

3. Di dare atto che la Valutazione di Impatto - DPIA verrà pubblicata sul sito del Comune di Foligno, sezione Amministrazione Trasparente – Altri contenuti – Prevenzione della Corruzione – Whistleblowing.

INFINE, considerata l'urgenza, si propone di dichiarare, con separata votazione, la deliberazione di cui alla presente proposta, immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D.Lgs n.267/2000.

30-01-2023

IL RESPONSABILE DEL PROCEDIMENTO

DOTT. PAOLO RICCIARELLI

AREA SEGRETERIA GENERALE

PROPOSTA DI DELIBERAZIONE: ART. 54BIS DEL D.LGS. 165/2001 - PROCEDIMENTO PER LE SEGNALAZIONI DI ILLECITI DA PARTE DI DIPENDENTI O COLLABORATORI DELL'ENTE - APPROVAZIONE DPIA (VALUTAZIONE DI IMPATTO) AI FINI DELLA NORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI DI CUI AL REG.UE 2016/679

PARERE DI REGOLARITA' TECNICA

Ai sensi dell'art. 49, comma 1 del D.Lgs. n. 267/2000, si esprime parere Favorevole alla regolarità tecnica della proposta di deliberazione.

Foligno, 30-01-2023

IL SEGRETARIO GENERALE

DOTT. PAOLO RICCIARELLI

Documento originale sottoscritto con firma digitale ai sensi dell' art.24 del D.Lgs. n. 82 del 07/03/2005

AREA SERVIZI FINANZIARI

PROPOSTA DI DELIBERAZIONE: ART. 54BIS DEL D.LGS. 165/2001 - PROCEDIMENTO PER LE SEGNALAZIONI DI ILLECITI DA PARTE DI DIPENDENTI O COLLABORATORI DELL'ENTE - APPROVAZIONE DPIA (VALUTAZIONE DI IMPATTO) AI FINI DELLA NORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI DI CUI AL REG.UE 2016/679

PARERE DI REGOLARITA' CONTABILE

Ai sensi dell’art. 49, comma 1 del D.Lgs. n. 267/2000, si esprime parere Non Necessario alla regolarità contabile della proposta di deliberazione.

Foligno, 30-01-2023

IL DIRIGENTE DELL'AREA SERVIZI FINANZIARI

MICHELA MARCHI

Documento originale sottoscritto con firma digitale ai sensi dell' art.24 del D.Lgs. n. 82 del 07/03/2005

Il presente atto viene letto, confermato e sottoscritto:

IL SINDACO	IL SEGRETARIO GENERALE
AVV. STEFANO ZUCCARINI	DOTT. PAOLO RICCIARELLI

COMUNE DI FOLIGNO

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi dell'art. 35 Reg. UE 2016/679 e della normativa vigente in materia di protezione dei dati personali.

Titolare del trattamento	Comune di Foligno
Responsabile del trattamento	Whistleblowing Solutions s.r.l.
Responsabile Protezione Dati	Anci Digitale S.p.A. la cui referente è l'Avv. Annalisa Luciani

Data di revisione 28-01-2023

SOMMARIO

1. Introduzione
2. Fonti normative
3. Definizioni
4. Descrizione del trattamento
5. Contesto:

A) Panoramica del trattamento
A) Dati, Processi e Risorse di supporto

6. Principi fondamentali:

A) Proporzionalità e necessità;
A) Misure a tutela degli interessati

7. Rischi:

A) Misure esistenti o pianificate;
A) Accesso illegittimo ai dati;
B) Modifiche indesiderate dei dati;
C) Perdita di dati;
D) Panoramica dei rischi

8. Parere degli interessati
9. Parere del Referente del R.P.D./D.P.O.

1. Introduzione

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 ha abrogato la direttiva 95/46/CE Regolamento generale sulla protezione dei dati – GDPR) è applicabile dal 25 maggio 2018.
L'art. 35 del GDPR prevede 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, può presentare un rischio elevato 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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".*
Ed ancora, il par. 3 prevede che la valutazione d'impatto sulla protezione dei dati di cui al par. 1 è richiesta in particolare nei seguenti casi: … lett. c) nel caso di *"sorveglianza sistematica su larga scala di zona accessibile al pubblico".*
Inoltre, al par. 7 il legislatore europeo stabilisce: "*la valutazione contiene 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".
Il presente documento rappresenta gli esiti della DPIA svolta nell'ambito del trattamento denominato **Whistleblowing** - di cui all'art. 54bis del D.Lgs. 165/2021 - effettuato dal Comune di Foligno.
La valutazione di impatto si riferisce alla valutazione dei rischi in cui potrebbero incorrere le libertà ed i diritti dei cittadini dall'utilizzo della piattaforma informatica gratuita ed è stata svolta dal Titolare del trattamento con il supporto del Segretario Generale Dott. Paolo Ricciarelli, in qualità di Responsabile della prevenzione della corruzione e della trasparenza (RPCT) e del Responsabile del Servizio Sistemi Informativi, Dott. Davide Castellucci.
Viene, inoltre, acquisito il parere del referente del Responsabile Protezione dati – DPO - Avv. Annalisa Luciani.
Il Titolare del trattamento provvederà: - all'adozione di politiche di controllo periodiche in riferimento ai dati oggetto del trattamento in questione e alle misure esistenti o pianificate (misure applicate ai dati, misure generali di sicurezza dei sistemi e misure organizzative); ad effettuare una precisa e rigorosa manutenzione dei sistemi; alla costante formazione del personale designato/autorizzato al trattamento dei dati.
La DPIA costituisce allegato al Registro dei trattamenti tenuto dal Comune di Foligno – approvato con deliberazione di Giunta Comunale n. 305 del 7/6/2019 e successive modifiche ed integrazioni - e viene pubblicata sul sito del Comune di Foligno, sezione Amministrazione Trasparente – Altri contenuti – Prevenzione della Corruzione - Whistleblowing.

2. Fonti normative

- Art. 54*bis* D.Lgs. 165/2001 (Testo Unico Pubblico Impiego);
- Deliberazione ANAC n. 469 del 09.6.2021;
- Regolamento UE n. 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"*;
- D.Lgs. n. 196 del 30 giugno 2003 recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;
- Linee Guida 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 adottate il 04 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017 dal Gruppo di Lavoro Articolo 29 per la Protezione dei Dati.

3. Definizioni

FONTE DI RISCHIO - Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (es.; amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio.
GRAVITA' - La gravità rappresenta l'entità del rischio e dipende principalmente dalla natura pregiudizievole del potenziale impatto.
IMPATTO - L'impatto rappresenta il grado di gravità dell'incidente che comporta la compromissione della riservatezza, integrità e disponibilità dei trattamenti e dei dati ad essi relativi.
PROBABILITA' - La probabilità esprime la possibilità che un rischio si realizzi e dipende principalmente dal livello di vulnerabilità delle risorse di supporto quando sottoposte alle minacce e dalla capacità delle fonti di rischio di sfruttare tali vulnerabilità.
MINACCIA – La minaccia è l'evento potenziale, cagionato ovvero accidentale, che comporterebbe il danno all'interessato.
VULNERABILITA' – La vulnerabilità è l'elemento di debolezza presente all'interno del sistema informativo o informatico sfruttabile dalla minaccia per la produzione del danno.
MISURE DI SICUREZZA - Soluzioni organizzative, tecnologiche o procedurali messe in atto dal Titolare del trattamento per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Reg. UE 679/2016.

4. Descrizione del trattamento

Per le caratteristiche di pervasità e intrusione nella sfera dei comportamenti personali, proprie del trattamento in esame, si rende necessaria l'effettuazione della presente valutazione di impatto del trattamento.
Per le modalità di funzionamento della piattaforma WhistleblowingPA si rimanda ai documenti allegati alla presente:

1. Scheda Sicurezza e tecnologia;

2. Accordo di collaborazione tra Transparency International Italia e Whistleblowing Solutions IS;
3. Certificazione ISO/IEC 27001:2017.

5. Contesto

A. PANORAMICA DEL TRATTAMENTO

1. Quale è il trattamento in considerazione?

Il trattamento in considerazione è denominato WHISTLEBLOWING e scaturisce da un Contratto di servizi sottoscritto tra il Comune di Foligno (Titolare del Trattamento) e Whistleblowing Solutions I.S. s.r.l. (Responsabile del Trattamento).
L'oggetto del suddetto contratto è la prestazione di un servizio di whistleblowing digitale consistente in fornitura di outsourcing di una piattaforma di whistleblowing digitale.
Il soggetto segnalante, ovvero colui che in ragione del proprio rapporto di lavoro presso l'Ente o presso soggetti che hanno rapporti di appalto/concessione con l'Ente sia venuto a conoscenza di condotte illecite, effettua la segnalazione in totale anonimato tecnologico accedendo alla piattaforma informatica gratuita.
I dati forniti dal soggetto segnalante vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

2. Quali sono le responsabilità connesse al trattamento?

In virtù del Contratto di Servizi sopra specificato, Whistleblowing Solutions I.S. s.r.l., in qualità di Responsabile del Trattamento, esegue operazioni di trattamento di dati personali per conto del Comune di Foligno.
Il Responsabile del Trattamento potrà avvalersi per l'attività di Archiviazione Hosting Cloud IASS della Seeweb s.r.l. in qualità di Sub-responsabile.
Il trattamento in questione oltre a dati comuni, potrebbe avere ad oggetto anche dati particolari e/o dati giudiziari (relativi a condanne penali e a reati) che potrebbero essere contenuti nella segnalazione e/o in atti e documenti ad essa allegati, riferiti agli interessati, ovvero a persone fisiche (identificate o identificabili) individuabili alternativamente nei soggetti:
- che inoltrano la segnalazione;
- indicati come possibili responsabili delle condotte illecite;
- a vario titolo coinvolti nelle vicende segnalate.

Il Comune di Foligno, in qualità di Titolare del trattamento, ha designato per il trattamento dei dati personali i Dirigenti dell'Ente, ai sensi dell'art. 2, comma quaterdecies, del D.Lgs. 196/2003 e, quanto alle funzioni in materia di anticorruzione e trasparenza, il Segretario Generale quale Responsabile della prevenzione della corruzione e per la trasparenza (RPCT), il quale svolge tale attività 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.

3. Ci sono standard applicabili al trattamento?

Per gli standard applicabili al trattamento si rinvia all'Art. 10 del Codice di comportamento integrativo del Comune di Foligno (approvato nell'ambito del PTPCT 2021-2023, approvato con deliberazione di Giunta n. 83 del 2021).

B. DATI, PROCESSI E RISORSE DI SUPPORTO

1. Quali sono i dati trattati?

Come già detto, oltre ai dati comuni potrebbero essere oggetto di trattamento anche dati particolari e/o dati giudiziari.
I soggetti nei confronti dei quali possono essere effettuate le segnalazioni sono:
-il Sindaco, i Consiglieri Comunali e gli Assessori dell'Ente;
- il Segretario generale;
- i Dirigente, i dipendenti di ruolo dell'Ente e i tirocinanti;
- i componenti dei Servizi di controllo interno;
- i consulenti e i collaboratori;
- i dipendenti di altre amministrazioni in posizione di comando, distacco o fuori ruolo presso l'Ente;
- i lavoratori e i collaboratori delle imprese fornitrici di beni o servizi presso l'Ente, nonché altri soggetti che a vario titolo interagiscono con l'Ente stesso.
Qualora il RPCT debba avvalersi di personale dell'Ente ai fini della gestione delle pratiche di segnalazione, tale personale per tale attività è appositamente autorizzato al trattamento ai sensi dell'art. 2-quadeterdecies d.lgs. 196/2003 e, di conseguenza, il suddetto personale dovrà attenersi al rispetto delle istruzioni impartite, nonché di quelle più specifiche, connesse ai particolari trattamenti, eventualmente di volta in volta fornite dal RPCT.
È fatto salvo, in ogni caso, l'adempimento, da parte del RPCT e/o dei soggetti che per ragioni di servizio debbano conoscere l'identità del segnalante, degli obblighi di legge cui non è opponibile il diritto all'anonimato del segnalante.
Con modalità tali da garantire comunque la riservatezza dell'identità del segnalante, il RPCT rende conto del numero di segnalazioni ricevute e del loro stato di avanzamento all'interno della relazione annuale di cui all'art. 1, comma 14, della legge n. 190/2012.
Il Titolare del Trattamento conserva i dati personali oggetto del trattamento denominato Whistleblowing per il periodo previsto dalla normativa vigente e, comunque, i dati personali raccolti a seguito della segnalazione sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a 18 mesi.
Il Responsabile del trattamento, all'atto della cessazione del Contratto, dovrà restituire al Comune di Foligno tutti gli eventuali dati personali di cui dovesse disporre (es. anagrafiche degli interessati, dati di contatto degli interessati) oppure, su richiesta del Titolare del trattamento provvedere alla loro distruzione, fornendone apposita attestazione, salvo eventuali esigenze di conservazione da parte del responsabile del trattamento in adempimento di obblighi normativi di cui fornirà contestuale attestazione al Comune di Foligno.

I dati personali raccolti a seguito della segnalazione, se del caso e nei limiti di legge, possono essere comunicati all'Autorità Giudiziaria, alla Corte dei Conti, al Dipartimento della Funzione Pubblica e all'ANAC.

2. **Quale è il ciclo di vita del trattamento dei dati (descrizione funzionale)?**

I dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite, delle quali sia venuto a conoscenza, commesse dai soggetti che a vario titolo interagiscono con il medesimo, vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti. La gestione e la preliminare verifica sulla fondatezza delle circostanze rappresentate nella segnalazione sono affidate al RPCT che vi provvede nel rispetto dei principi di imparzialità e riservatezza effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati. Qualora, all'esito di tale verifica di delibazione, si ravvisino elementi di non manifesta infondatezza del fatto segnalato, il Responsabile provvederà a trasmettere l'esito dell'accertamento per approfondimenti istruttori o per l'adozione dei provvedimenti di competenza:
a) al dirigente responsabile del Servizio Risorse Umane, nonché al Responsabile dell'Area organizzativa di appartenenza dell'autore della violazione, affinché sia espletato, ove ne ricorrano i presupposti, l'esercizio dell'azione disciplinare;
b) agli organi e alle strutture competenti dell'Ente affinché adottino gli eventuali ulteriori provvedimenti e/o azioni ritenuti necessari, anche a tutela dell'Ente stesso;
c) se del caso, all'Autorità Giudiziaria, alla Corte dei conti, al Dipartimento della Funzione Pubblica e all'ANAC. In tali casi, nell'ambito dell'eventuale procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale; nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria; nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa; in caso contrario, il segnalante può opporsi alla rivelazione della propria identità, di conseguenza il procedimento deve essere archiviato.
Pertanto, i dati non verranno diffusi, ma comunicati secondo le previsioni della normativa vigente.
Non vi è trasferimento all'estero dei dati personali trattati.
L'interessato può esercitare i diritti di cui agli artt. 15 e segg. del GDPR tramite richiesta mail all'indirizzo segretario@comune.foligno.pg.it o all'indirizzo pec del referente del Responsabile della Protezione dei dati - DPO avvannalisaluciani@puntopec.it.

3. **Quali sono le risorse di supporto dei dati?**

Le risorse impiegate per il trattamento in esame comprendono:

N.2 connessioni internet di tipo SPC (Sistema Pubblico di Connettività che **è la rete che collega tra loro tutte le pubbliche amministrazioni italiane**, consentendo loro di condividere e scambiare dati e risorse informative);
N. 2 firewall (uno per ogni connessione internet SPC) collegati in HA (Alta affidabilità) e ridondanti;
N. 36 switch (apparati di rete) collegati tra loro in Fibra ottica;

N. 12 Server Fisici + N. 35 Server Virtuali backuppati fra di loro per rendere resiliente e resistente il sistema informativo comunale;
N.5 Server virtuali in Cloud certificato AGID per rendere sicuri i dati su loro contenuti;
N. 5 Specialisti informatici che afferiscono al Servizio Sistemi Informativi Comunale.

6. Principi fondamentali

A) PROPORZIONALITA' E NECESSITA'

1. Gli scopi del trattamento sono specifici, espliciti e legittimi?

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 vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti (indicati al par. 5 delle istruzioni).
Gli scopi perseguiti con il trattamento denominato "Wistleblowing" risultano, in termini generali, leciti, ai sensi dell'art. 5.1.a) Reg. UE 679/2016.

2. Quali sono le basi legali che rendono lecito il trattamento?

Le basi legali che rendono lecito il trattamento sono:

- Necessità del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1 lett. e) Reg. UE 679/2016);

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

La raccolta dei dati viene effettuata nel rispetto del *principio di minimizzazione dei dati,* di cui all'art. 5.1 lett. c) Reg. UE 679/2016, ovvero si svolge in maniera tale da ridurre la gravità dei rischi limitando la raccolta di dati personali al minimo necessario per la specifica finalità.

4. I dati raccolti sono esatti e aggiornati?

Ai sensi dell'art. 5 par. 1 lett. d) Reg. UE 2016/679, i dati trattati sono esatti e, se necessario, aggiornati.
Inoltre, Il Comune di Foligno adotta tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

5. Quale è il periodo di conservazione dei dati?

I dati personali trattati vengono conservati nel rispetto del principio di "limitazione della conservazione" di cui all'art. 5.1 lett. e) Reg. UE 679/2016.
Come detto, il Responsabile del trattamento all'atto della cessazione del Contratto dovrà restituire al Comune di Foligno tutti gli eventuali dati personali di cui dovesse disporre o, in alternativa, su richiesta del Titolare del trattamento provvedere alla loro distruzione,

fornendone apposita attestazione, salvo eventuali esigenze di conservazione in adempimento di obblighi normativi gravanti sullo stesso Responsabile del trattamento, di cui fornirà contestuale attestazione al Comune di Foligno.
Quest'ultimo conserva i dati personali oggetto del trattamento in questione per il periodo previsto dalla normativa vigente e, comunque, i dati personali raccolti a seguito della segnalazione sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a 18 mesi.

B) MISURE A TUTELA DEGLI INTERESSATI

1. **Come sono informati del trattamento gli interessati?**

L'informativa resa ai soggetti interessati ai sensi dell'art. 13 del Reg. UE 679/2016, è pubblicata sul sito del Comune di Foligno - Sezione Amministrazione Trasparente – Altri contenuti – Prevenzione e corruzione – Whistleblowing Segnalazioni condotte illecite (Allegato 4)

2. **Ove applicabile come si ottiene il consenso degli interessati?**

Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità; in caso contrario il procedimento dovrà essere archiviato.

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

Gli interessati possono esercitare il diritto di accesso ai sensi dell'art. 15 Reg. UE 679/2016 mediante il deposito di specifica istanza. Ai sensi dell'art. 20.3 Reg. UE 679/2016, il diritto alla portabilità dei dati "non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento".

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

Gli interessati hanno diritto di ottenere la rettifica dei dati personali, ai sensi dell'art. 16 Reg. UE 679/2016, mediante deposito di specifica istanza.
L'esercizio del diritto di cancellazione ("diritto all'oblio") ai sensi dell'art. 17.3 lett. b), non è esercitabile in riferimento al trattamento in esame.

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

Gli interessati hanno diritto di esercitare i loro diritti di limitazione e di opposizione presentando apposita istanza al Responsabile della prevenzione della corruzione e della trasparenza (R.P.C.T.) mediante il deposito di specifica istanza.

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

Sì. Gli obblighi di Wistleblowing Solutions I.S. s.r.l., in qualità di Responsabile del Trattamento, sono definiti nel contratto sottoscritto in data 06.12.2020 che si allega alla presente Valutazione di Impatto (Allegato 5).

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

I dati non vengono trasferiti all'estero.

7. Rischi

A) MISURE ESISTENTI O PIANIFICATE

MISURE APPLICATE AI DATI:

- ***CRITTOGRAFIA -*** I Gestionali comunali sono utilizzati attraverso il WEB ed utilizzano il protocollo **HyperText Transfer Protocol over Secure Socket Layer** (**HTTPS**) che è un protocollo per la comunicazione sicura attraverso una rete di computer utilizzato su Internet. Consiste nella comunicazione tramite il protocollo HTTP (Hypertext Transfer Protocol) all'interno di una connessione criptata, tramite crittografia asimmetrica, dal Transport Layer Security (TLS) o dal suo predecessore, Secure Sockets Layer (SSL) fornendo come requisiti chiave un'autenticazione del sito web visitato, protezione della privacy (riservatezza o confidenzialità), integrità dei dati scambiati tra le parti comunicanti.
  Infatti risulta che ogni server WEB comunale che espone un gestionale o un servizio è provvisto di certificato SSL che in maniera automatica cripta le informazioni scambiate tra il client ed il server.
  Lo smart-working viene implementato attraverso il Servizio **Remote Desktop Services** di Microsoft (**Remote Desktop Gateway)**. Tale servizio installa sul Server preposto il ruolo di **Network Policy Server**, il web server **IIS** e la funzione **RPC over HTTP**, che si occuperà di incapsulare il traffico RDP in un tunnel protetto e criptato attraverso il protocollo di comunicazione sicuro HTTPS.

- ***ANONIMIZZAZIONE:*** Il Comune di Foligno usa Web Analytics Italia (WAI) è una piattaforma nazionale di raccolta e analisi dei dati statistici relativi al traffico dei siti e servizi digitali della Pubblica Amministrazione italiana.
  WAI consente di uniformare la raccolta di tali dati, semplificare l'accesso alle statistiche sul traffico e sul comportamento degli utenti che usano siti e servizi digitali istituzionali, fornire agli operatori della PA strumenti *ad hoc* per agevolare la comprensione di tali informazioni, con l'obiettivo finale di ottimizzare in maniera continua l'esperienza utente. La piattaforma espone inoltre pubblicamente, e in maniera aggregata, alcuni dei dati che riguardano la fruizione dei servizi digitali della PA da parte dei cittadini. WAI utilizza di default il sistema di anonimizzazione

dell'indirizzo IP degli utenti, quindi non sarà necessario intraprendere altre azioni per rendere anonime le visite.

- ***PARTIZIONAMENTO**:* Tutti dati vengono archiviati in cartelle in base al servizio con accesso autorizzato solo ai dipendenti del servizio.

- ***CONTROLLO DEGLI ACCESSI LOGICI**:* Rilascio di credenziali con ACL (Access control list) su un dominio di Microsoft Active Directory 5 lunghezza minima password 8, politiche password: almeno una maiuscola una minuscola e un numero, validità password 90 giorni, numero 5 tentativi prima del blocco dell'account.

- ***TRACCIABILITA'**:* I Log dei Server e dei firewall vengono conservati in una cartella su un server di rete sicuro accessibile solo con credenziali da Amministratore.

- ***ARCHIVIAZIONE:*** Tutti gli archivi sono conservati su server sicuri, aggiornati e dietro firewall per sventare attacchi dall'esterno, politiche di backup vengono attuate in maniera sistematica ed esaustiva.
  I dati e gli archivi del gestionale comunale vengono mandati in conservazione sostitutiva in maniera automatica e usando protocolli di comunicazione sicuri.

- ***SICUREZZA DEI DOCUMENTI CARTACEI**:* Le stampe inviate alle stampanti non vengono subito stampate ma attendono l'inserimento di una password da parte dell'operatore affinché nessun altro, tranne l'operatore stesso, possa consultarle e/o sottrarle.

- ***MINIMIZZAZIONE DEI DATI**:* Usando sistemi centralizzati e piattaforme di autenticazione centralizzate si riduce la richiesta del dato stesso e si riduce l'accesso stesso al dato.

MISURE GENERALI DI SICUREZZA DEI SISTEMI:

- ***VULNERABILITA'**:* La rete comunale è protetta verso l'esterno da Firewall che impedisce l'accesso a malintenzionati. Internamente invece tutti i dipendenti sono riconosciuti da credenziali personali. Tutti i PC vengono aggiornati in base a quanto richiesto dal fornitore/produttore, inoltre i dati vengono duplicati su più server. I server sono fisicamente in una stanza chiusa e le chiavi sono in possesso solo dei dipendenti dei servizi informatici e della portineria.

- ***LOTTA CONTRO IL MALWARE:*** Tutti i PC sono dotati di software antivirus e antimalware, inoltre tali software sono gestiti in maniera centralizzata affinché la presenza di un virus o di un malware sia subito scoperto e siano attivate in maniera tempestiva le misure per contenere eventuali incidenti.

- ***GESTIONE POSTAZIONI:*** Uso di credenziali personali, software antivirus e antimalware, spazio di rete condiviso e protetto, aggiornamenti costanti del sistema operativo, logging degli accessi ai PC.

- ***SICUREZZA SITI WEB**:* Ogni server WEB comunale che espone un gestionale o un servizio è provvisto di certificato SSL (TSL) che in maniera automatica cripta le informazioni scambiate tra il client ed il server.

- ***BACKUP:*** Politiche di Backup sicuri e protetti giornalieri, settimanali e mensili anche in siti diversi**.**

- ***MANUTENZIONE**:* Manutenzione dei PC dai dipendenti interni comunali, manutenzione eseguita anche da remoto ed in maniera automatica.

- ***CONTRATTO CON IL RESPONSABILE DEL TRATTAMENTO*** Il Comune di Foligno ha sottoscritto con Whistleblowing Solutions I.S. s.r.l. un accordo in merito al trattamento di dati personali ai sensi dell'art. 28 del Reg. UE 2016/679 (Allegato 5); inoltre, il Responsabile del Trattamento dati (Whistleblowing Solutions I.S. s.r.l) ha sottoscritto con Associazione Trasparency International Italia, un Accordo di collaborazione (Allegato 2).

- ***SICUREZZA DEI CANALI INFORMATICI*** Il Comune di Foligno, ha implementato sistemi di protezione adeguati a seconda del tipo di rete sulla quale il trattamento è effettuato (isolata, privata o internet).

*MISURE ORGANIZZATIVE**:***

- ***POLITICA DI TUTELA DELLA PRIVACY*** Il Comune di Foligno ha provveduto:

- alla designazione del Responsabile Protezione Dati (DPO), ai sensi dell'art. 37 Reg. Ue 2016/679;
- alla designazione e delega dei soggetti di cui all'art. 2quaterdecies D.Lgs. 196/2003 ai fini della nomina da parte degli stessi dei Responsabili del trattamento dei dati personali;

provvede, inoltre:

- alla tenuta del Registro delle attività di trattamento, delle informative, delle nomine dei Responsabili del trattamento, delle valutazioni di impatto (ove necessarie);
- alla formazione dei soggetti autorizzati/delegati al trattamento dei dati.

- ***GESTIONE DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI DEI DATI PERSONALI*** Esistenza di un'organizzazione operativa (CERT (Computer Emergency Response Team) Umbria di PuntoZero scarl, società in house del Comune) per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni, ecc.)

- ***GESTIONE DEL PERSONALE*** Il Titolare del trattamento ha provveduto e provvede costantemente alla formazione dei soggetti designati/autorizzati al trattamento dei dati personali.

  I soggetti designati/autorizzati al trattamento dei dati sono nominati con specifici atti, come da Regolamento comunale e sono istruiti e formati sul corretto trattamento.

- ***GESTIONE DEI TERZI CHE ACCEDONO AI DATI*** L'accesso ai dati da parte di terzi è legittimato da contratti o convenzioni. Gli accessi da parte dei terzi sono tracciati ed autorizzati dai sistemi informativi comunali con utenze personali e a scadenza.

- ***VIGILANZA SULLA PROTEZIONE DEI DATI*** Il Titolare del trattamento svolge una costante attività di verifica dei trattamenti effettuati e se necessario provvede all'aggiornamento del Registro delle attività di trattamento, delle Valutazioni di impatto, delle informative.

B. ACCESSO ILLEGITTIMO AI DATI (Indisponibilità dei dati – distruzione, perdita, furto)

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

Qualora il rischio si dovesse concretizzare gli interessati potrebbero sperimentare IMPATTI LIMITATI, ovvero, inconvenienti significativi, superabili nonostante alcune difficoltà.

2. **Quali sono le principali minacce che potrebbero concretizzare il rischio?**

Le minacce principali che potrebbero concretizzare il rischio sono le seguenti:

Attacco Hacker attraverso la rete internet;
Attacco Hacker attraverso la rete dati interna;
Attacco Hacker attraverso la posta elettronica;
Attacco Hacker attraverso Virus o Malware.

3. **Quali sono le fonti di rischio?**

Le fonti di rischio potrebbero essere rappresentate da una persona, interna o esterna all'Ente, operante in via accidentale o intenzionale (es.: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio.
Le motivazioni potrebbero essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

4. **Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**

Tutte le misure tecniche e organizzative messe in atto dal Titolare del trattamento, sopra specificate, contribuiscono a mitigare il rischio.

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

La gravità del rischio stimata è: LIMITATA

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

La probabilità del rischio stimata è: TRASCURABILE

C. MODIFICHE INDESIDERATE DEI DATI (Integrità dei dati – alterazione, modifica).

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

Qualora il rischio si dovesse concretizzare gli interessati potrebbero sperimentare IMPATTI LIMITATI, ovvero, inconvenienti significativi, superabili nonostante alcune difficoltà.

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

Come già detto precedentemente le minacce principali sono le seguenti:

Attacco Hacker attraverso la rete internet;
Attacco Hacker attraverso la rete dati interna;
Attacco Hacker attraverso la posta elettronica;
Attacco Hacker attraverso Virus o Malware.

3. Quali sono le fonti di rischio?

Le fonti di rischio potrebbero essere rappresentate da una persona, interna o esterna all'Ente, operante in via accidentale o intenzionale (es.: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio. Le motivazioni potrebbero essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

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

Tutte le misure tecniche e organizzative messe in atto adottate dal Titolare del trattamento, sopra specificate, contribuiscono a mitigare il rischio.

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

La gravità del rischio stimata è: LIMITATA.

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

La probabilità del rischio stimata è: TRASCURABILE.

D. PERDITA DI DATI (Riservatezza dei dati – accesso abusivo, trattamento non conforme)

1. Quali sarebbero i principali impatti sugli interessati se il rischio dovesse concretizzarsi?

Qualora il rischio si dovesse concretizzare gli interessati potrebbero sperimentare un IMPATTO LIMITATO, ovvero, inconvenienti significativi, superabili nonostante alcune difficoltà.
In caso di accesso illegittimo alle immagini si ritiene non si concretizzi un danno rilevante, in quanto il soggetto prenderebbe semplicemente visione.

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

Come già detto precedentemente le minacce principali sono le seguenti:

Attacco Hacker attraverso la rete internet;
Attacco Hacker attraverso la rete dati interna;
Attacco Hacker attraverso la posta elettronica;
Attacco Hacker attraverso Virus o Malware.

3. Quali sono le fonti di rischio?

Le fonti di rischio potrebbero essere rappresentate da una persona, interna o esterna all'Ente, operante in via accidentale o intenzionale (es.: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio. Le motivazioni potrebbero essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

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

Tutte le misure tecniche e organizzative messe in atto adottate dal Titolare del trattamento, sopra specificate, contribuiscono a mitigare il rischio.

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

La gravità del rischio stimata è: LIMITATA

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

La probabilità del rischio stimata è: TRASCURABILE

8. Parere degli interessati

Non è stato ritenuto necessario, anche in considerazione degli esiti della presente valutazione, acquisire il parere dei potenziali interessati.

9. Parere del R.P.D./D.P.O.

A seguito di attenta analisi del presente documento, visto l'art. 39 par. 1 lett. C) del Reg. UE 2016/679, la sottoscritta Avv. Annalisa Luciani, in qualità di referente del D.P.O. designato, Anci Digitale S.p.A., tenuto conto:
- dell'adozione da parte del Titolare del trattamento di politiche di controllo periodiche in riferimento ai dati oggetto del trattamento in questione e alle misure esistenti o pianificate (misure applicate ai dati, misure generali di sicurezza dei sistemi e misure organizzative);
- della esecuzione di una precisa e rigorosa manutenzione dei sistemi;
- della costante formazione del personale designato/autorizzato al trattamento dei dati,
ritiene che i rischi per i diritti e le libertà fondamentali degli interessati, relativi ai trattamenti in discorso, possano essere qualificati come medio-bassi.
Pertanto, nel complesso, alla data odierna, non si ritiene esistente un "rischio elevato" come inteso dall'art. 35 Reg. UE 2016/679.
Per tale ragione, non si ritiene necessario procedere con la Consultazione preventiva ex art. 36 Reg. UE 2016/679.
Il presente documento viene sottoscritto digitalmente dal DPO Avv. Annalisa Luciani.

*** * ***

Si allegano alla presente Valutazione di impatto (con oscuramento dei dati personali):

1. Scheda Sicurezza e tecnologia;
2. Accordo di collaborazione tra Transparency International Italia e Whistleblowing Solutions Is;
3. Certificazione ISO/IEC 27001:2017.
4. Informativa ai sensi dell'art. 13 Reg. UE 679/2016
5. Accordo in merito al trattamento dei dati personali tra Comune di Foligno e Whistleblowing Solutions I.S. s.r.l. (Nomina Responsabile del trattamento).

WhistleblowingPA: piattaforma per la segnalazione di illeciti all'interno delle Pubbliche Amministrazioni

Nell'ottobre 2018 Transparency Italia e Centro Hermes hanno lanciato il progetto WhistleblowingPA allo scopo di fornire a tutte le amministrazioni pubbliche una piattaforma informatica gratuita. Questa è conforme alla legge 179/2017 a tutela dei segnalanti e alle linee guida dell'Autorità Nazionale Anticorruzione (ANAC).

Il software GlobaLeaks

Soluzione gratuita e alternativa all'applicativo rilasciato da ANAC all'inizio del 2019, GlobaLeaks garantisce la possibilità di segnalare in totale anonimato tecnologico e, da parte delle amministrazioni, di instaurare un dialogo con il segnalante utile a circostanziare i fatti emersi. Una volta creata una piattaforma su WhistleblowingPA ne sono garantiti il mantenimento e l'aggiornamento senza la necessità di alcun intervento tecnico esterno o interno all'ente.

Sicurezza e anonimato del software

1. misure di sicurezza applicate dal software globaleaks:

https://docs.google.com/document/u/1/d/1niYFyEar1FUmStC03OidYAIfVJf18ErUFwSWCmWBhcA/pub
https://docs.google.com/document/u/1/d/1SMSiAry7x5XY9nY8GAejJD75NWg7bp7M1PwXSiwy62U/pub
https://github.com/globaleaks/GlobaLeaks/wiki/Operating-system-security
https://github.com/globaleaks/GlobaLeaks/wiki/Encryption

Le principali caratteristiche di sicurezza del framework sono:

- Supporto nativo per trasporto sicuro HTTPS con rating A+ da SSL Labs
- Supporto nativo a Let's Encrypt
- Piena integrazione della tecnologia Tor, stato dell'arte in materia di comunicazioni sicure ed anonime;
- Piena integrazione della tecnologia PGP come standard per la cifratura di email e file allegati;
- Firewall integrato;
- Application Sandboxing integrato;
- Completo set di funzionalità anti-DoS ed anti-Bot;

- Il software ha già ricevuto 4 analisi di sicurezza indipendenti ed è continuamente oggetto di peer-review dalla comunità di sviluppatori ed analisti indipendenti: (https://github.com/globaleaks/GlobaLeaks/wiki/Penetration-Tests).

2. test di sicurezza effettuati dal software globaleaks: https://github.com/globaleaks/GlobaLeaks/wiki/Penetration-Tests

Servizio di Hosting

Il Servizio di Whistleblowing Digitale offerto consiste nella fornitura di un sistema SaaS (Software as a Service) configurato e personalizzato. Non è previsto alcun tipo di fornitura tecnologica fisica, nè costi di licenza per il cliente.

Il servizio è reso disponibile su infrastruttura ridondata di WBS. L'infrastruttura gestita da esegue l'applicativo GlobaLeaks accessibile tramite il dominio segnalazioni.nomecliente.it, di proprietà del cliente. L'infrastruttura sarà inoltre raggiungibile tramite Tor Onion Service il cui indirizzo verrà fornito a seguito dell'attivazione del servizio.

Le piattaforme del progetto WhistleblowingPA si trovano sui Datacenter della società Seeweb (https://www.seeweb.it/), in particolare a Milano e. per ridondanza, presso Frosinone.

Sviluppo, gestione e manutenzione della piattaforma

Whistleblowing Solutions I.S. s.r.l.

Sede legale in Milano - Viale Aretusa 34, in persona del legale rappresentante pro tempore.

ACCORDO DI COLLABORAZIONE

TRA

TRANSPARENCY INTERNATIONAL ITALIA

E

WHISTLEBLOWING SOLUTIONS IS

PER LA GESTIONE INFORMATICA DELLA PIATTAFORMA DI WHISTLEBLOWING ANTICORRUZIONE GRATUITA PER TUTTE LE PUBBLICHE AMMINISTRAZIONI ITALIANE

Associazione Transparency International Italia (di seguito, TI-It) – organizzazione non governativa contro la corruzione, con sede in Piazzale Carlo Maciachini 11, 20159, Milano, nella persona del Presidente XXXXXXXXXX

e

Whistleblowing Solutions I.S. S.r.l. (in seguito WBS), con sede in Viale Aretusa, 34, in persona di XXXXXXXXXXX

PREMESSO CHE

- TI-It ha come obiettivo la realizzazione di una piattaforma digitale di whistleblowing gratuita, a disposizione di tutta la pubblica amministrazione italiana senza oneri, frutto della collaborazione ed esperienza del team del software GlobaLeaks (Associazione Hermes) e TI-it.

- La piattaforma erogata sarà gratuita per tutte le pubbliche amministrazioni, inclusiva di supporto best-effort da parte di WBS e TI-it per le rispettive aree di competenza, meglio identificate in seguito.

- Il progetto prevede una dinamica di sostenibilità economica tramite la sollecitazione di contributi economici liberali da parte di pubbliche amministrazioni.

- TI-It ai sensi del Regolamento UE 2016/679 opera in qualità di Titolare del trattamento.

- Whistleblowing Solutions IS è una start-up innovativa a vocazione sociale nata per soddisfare la crescente richiesta di supporto software per il contrasto alla corruzione ed è parte integrante della comunità open source GlobaLeaks oltre ad essere partecipata al 40% dall’Associazione Hermes.

CONVENGONO E STIPULANO QUANTO SEGUE:

ARTICOLO 1

Tutto quanto in premessa costituisce parte integrante e sostanziale del presente protocollo.

ARTICOLO 2
OBIETTIVO

Il presente Accordo di collaborazione ha come obiettivo l'affidamento della gestione della piattaforma digitale di whistleblowing gratuita, a disposizione di tutta la pubblica amministrazione italiana senza oneri, frutto della collaborazione ed esperienza del team del software GlobaLeaks (Associazione Hermes) e TI-it.

ARTICOLO 3
MODALITÀ' DI COLLABORAZIONE

Hermes e TI-it operano nei rispettivi ambiti di competenza esclusivamente per la promozione e divulgazione del progetto a fini sociali in particolare attraverso la gestione del sito web https://www.whistleblowing.it e l'utilizzo dei rispettivi canali informativi compresi i social network.

WBS si occuperà del tutto autonomamente dell'erogazione e della gestione della piattaforma gratuita impegnandosi in particolare a ottemperare ai seguenti punti:

- Sito web della iniziativa
    - Setup e manutenzione tecnica

- Server e software di erogazione della piattaforma di whistleblowing
    - Il setup tecnico infrastrutturale

- Supporto best-effort tramite Forum web
    - Realizzazione e manutenzione infrastruttura di forum web

ARTICOLO 4
REFERENTI

Le Parti designano ciascuna un Referente per l'esecuzione del presente Accordo.

I Referenti designati dalle Parti sono:
a) per TI-It: XXXXXXXXXXXXXXXX

b) per WBS: XXXXXXXXXXXXXXXXXX

Ciascuna Parte si riserva il diritto di sostituire i propri Referenti, dandone tempestiva comunicazione alla controparte.

ARTICOLO 5
DURATA

Il presente Protocollo entra in vigore il giorno successivo alla data della sua sottoscrizione, ha durata annuale e si rinnova automaticamente, fatto salvo comunicazione scritta da una delle parti entro 30 giorni dalla data di termine del presente accordo.

ARTICOLO 6
ONERI

L'attività oggetto del presente accordo viene effettuata a titolo gratuito.

ARTICOLO 7
TRATTAMENTO DEI DATI PERSONALI

TI-it effetua operazioni di trattamento di dati personali determinando le finalità e i mezzi del trattamento con particolare riferimento alle attività svolte per la gestione dei dati personali relativi all'iniziativa.
TI-it in qualità di Titolare del trattamento nomina WBS come Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679 in relazione a:

- ai dati inerenti la navigazione web del sito https://www.whistleblowing.it. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer e dei terminali utilizzati dagli utenti, gli indirizzi in notazione URI/URL (Uniform Resource Identifier/Locator) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. I dati di navigazione non persistono per più di 90 (novanta) giorni e vengono cancellati immediatamente dopo la loro aggregazione (salve eventuali necessità di accertamento di reati da parte dell'Autorità giudiziaria).
- operazioni di trattamento di dati personali riferiti ai dati necessari per l'erogazione dei servizi pattuiti tra le parti. In particolare dati identificativi e di contatto dei referenti dei clienti finali che attivano il servizio di digital whistleblowing. Tali dati sono afferenti principalmente ai Responsabili Anticorruzione nelle PA e in altre funzioni di controllo stabilite dalle normative in ambito privato (es. OdV 231, Internal Audit, Compliance, Risk Management, ecc.). La conservazione dei dati è di 18 mesi dopo la disattivazione del servizio.

- operazioni di trattamento di dati personali riferiti ai dati necessari per l'erogazione dei servizi pattuiti tra le parti. In particolare l'acquisizione e l'archiviazione delle segnalazioni può dar luogo a trattamenti di dati personali appartenenti anche a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti agli interessati, ovvero alle persone fisiche (identificate o identificabili) che inoltrano una segnalazione o a quelle indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate (art. 4, par. 1, nn. 1) e 2), del Regolamento.

In relazione a ciò WBS si impegna a:

a) svolgere le operazioni di trattamento di dati personali in conformità ai principi e alla regolamentazione previsti dalla normativa vigente in materia di protezione dei dati personali;
b) eseguire le istruzioni impartite dal Titolare, evitando attività di trattamento non conformi alle predette istruzioni o volte a perseguire finalità diverse da quelle oggetto del presente accordo;
c) non divulgare o rendere noti a terzi i dati personali e adottare le misure organizzative e tecniche necessarie per assicurare la massima riservatezza;
d) garantire che l'accesso ai dati personali da parte del personale avvenga solo sulla base del principio di stretta necessità, provvedendo a individuare e designare quali incaricati del trattamento le persone fisiche (dipendenti e/o collaboratori) autorizzate al trattamento dei dati personali per le suddette finalità, impegnando gli stessi con idonei vincoli di riservatezza;
e) informare il Titolare, entro 48 ore ore dal momento in cui ne è venuto a conoscenza, di qualsiasi violazione o rischio di violazione concernente i dati personali di cui WBS è venuta a conoscenza nello svolgimento dei servizi;
f) adottare le misure di sicurezza misura idonee a prevenire i rischi di distruzione, perdita, anche accidentale, dei dati personali nonché di accesso non autorizzato o trattamento illecito dei medesimi come previsto dall'art. 32 del Regolamento UE 2016/679. In relazione a ciò WBS si impegna a scegliere gli amministratori di sistema tra quei soggetti dotati di esperienza, capacità ed affidabilità, in grado di garantire il pieno rispetto della normativa italiana in materia di protezione dei dati personali, ivi compreso il profilo relativo alla sicurezza, nominare gli amministratori di sistema individualmente, elencando analiticamente gli ambiti di operatività consentiti a ciascun amministratore di sistema in relazione al proprio profilo di autenticazione, tenere un elenco aggiornato dei soggetti nominati amministratori di sistema e, su richiesta, mettere tale elenco a disposizione del Committente e/o delle autorità competenti e a a verificare regolarmente l'idoneità delle misure adottate.

E' consentito a WBS di avvalersi di soggetti terzi ai fini della prestazione dei servizi senza il preventivo consenso scritto del Titolare. WBS si impegna a prevedere nel contratto con il subappaltatore garanzie e obblighi analoghi a quelli di cui al presente accordo. il Responsabile del trattamento dichiara di avvalersi del Subresponsabile Seeweb S.r.l., il quale si intende

approvato dal Titolare del trattamento. Qualora WBS intenda sostituire oppure inserire nuovi Subresponsabili, dovrà informare il Titolare preventivamente e per iscritto.

WBS riconosce e accetta che il Titolare, possa controllare le operazioni di trattamento di dati personali svolte da WBS, come anche le misure di sicurezza attuate da quest'ultimo per le finalità di cui al presente contratto, anche mediante appositi audit da concordarsi preventivamente nel rispetto delle reciproche esigenze lavorative.

ARTICOLO 8
PROPRIETA' E UTILIZZO

Salvo quanto disposto dalla legge in materia di diritto d'autore e proprietà industriale e fermo restando il diritto morale degli inventori ad essere riconosciuti tali, il materiale, i progetti o altre creazioni intellettuali inventate, predisposte o realizzate con l'apporto congiunto delle Parti in occasione dell'esecuzione del presente accordo, sono in contitolarità delle Parti, in Italia e all'Estero.
Le Parti si impegnano a tutelare e promuovere l'immagine dell'iniziativa comune e la propria. In particolare, i loghi delle parti potranno essere utilizzati nell'ambito delle attività comuni oggetto del presente accordo. Il presente accordo non implica alcuna spendita del nome, e/o concessione e/o utilizzo del marchio e dell'identità visiva delle parti per fini commerciali, e/o pubblicitari. Tale utilizzo, straordinario e/o estraneo all'azione istituzionale, dovrà esser regolato da specifici accordi, approvati dagli organi competenti e compatibili con la tutela dell'immagine. L'utilizzazione dei loghi, straordinaria o estranea all'azione istituzionale corrispondente all'oggetto del presente accordo, richiederà il consenso della Parte interessata, nel rispetto delle relative procedure interne.

ARTICOLO 9
CONTROVERSIE

In caso di controversia nell'interpretazione o esecuzione del presente accordo, la questione verrà in prima istanza sottoposta a mediazione, secondo le previsioni del D.Lgs. 28/2010 e successivi decreti di attuazione, presso l'Organismo di conciliazione della Camera Arbitrale di Milano. Le parti si obbligano a ricorrere alla mediazione prima di dare avvio a qualsiasi procedimento arbitrale o giudiziale. Per qualsiasi controversia non risolvibile attraverso la Camera Arbitrale viene eletto il Foro di Milano, quale foro competente

ARTICOLO 10
COMUNICAZIONI

Tutte le comunicazioni fra le Parti devono essere inviate, salva diversa espressa previsione, per iscritto ai rispettivi indirizzi di posta elettronica, qui di seguito precisati:
per TI-It: info@transparency.it
per WBS: accounting@whistleblowingsolutions.it

Milano, lì 10/11/2020

IL PRESIDENTE DI TRANSPARENCY INTERNATIONAL
ITALIA XXXXXXXXXXXXXXXXXXXX

L’AMMINISTRATORE DELEGATO DI WHISTLEBLOWING SOLUTIONS
IS XXXXXXXXXXXXXXXXXXXX

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.

CERTIFICATO n° / *CERTIFICATE n°* **50030**

SI CERTIFICA CHE L'ORGANIZZAZIONE
WE HEREBY CERTIFY THAT THE ORGANIZATION

WHISTLEBLOWING SOLUTIONS IMPRESA SOCIALE S.r.l.

For information concerning the validity of the certificate, you can visit the site www.certiquality.it

The validity this certificate depends on annual audit and on a complete review every three years of the Management System.

VIALE ARETUSA, 34 - 20147 MILANO MI

NELLE SEGUENTI UNITA' OPERATIVE / IN THE FOLLOWING OPERATIVE UNITS

VIA VITRUVIO, 1 - 20124 MILANO MI

HA ATTUATO E MANTIENE UN SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI CHE E' CONFORME ALLA NORMA
HAS IMPLEMENTED AND MAINTAINS AN INFORMATION SECURITY MANAGEMENT SYSTEM WHICH COMPLIES WITH THE FOLLOWING STANDARD

UNI CEI EN ISO/IEC 27001:2017

PER LE SEGUENTI ATTIVITÀ / *FOR THE FOLLOWING ACTIVITIES*

SETTORE CODE **IAF | 33**

Erogazione di Servizi SAAS di Whistleblowing Digitale.
Il Sistema di Gestione della sicurezza delle informazioni soddisfa i criteri contenuti nelle seguenti Linee Guida: ISO/IEC 27017:2015 e ISO/IEC 27018:2019.Certificato emesso in accordo con la versione della dichiarazione di applicabilità del 03/02/2020.

Provision of SAAS Digital Whistleblowing Services.
The Information Security Management System meets the criteria contained in the following Guidelines: ISO /IEC 27017: 2015 and ISO / IEC 27018: 2019.Certificate issued in compliance with the version of statement of applicability of 03/02/2020.

CERTIFICATO EMESSO IN ACCORDO CON L'ULTIMA VERSIONE DELLA DICHIARAZIONE DELL'APPLICABILITA'
CERTIFICATE ISSUED IN COMPLIANCE WITH THE LAST VERSION OF THE STATEMENT OF APPLICABILITY

IL PRESENTE CERTIFICATO È SOGGETTO AL RISPETTO DEL REGOLAMENTO PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE
THE USE AND THE VALIDITY OF THE CERTIFICATE SHALL SATISFY THE REQUIREMENTS OF THE RULES FOR THE CERTIFICATION OF MANAGEMENT SYSTEMS

PRIMA EMISSIONE *FIRST ISSUE*	12/03/2020
DATA DELIBERA *DECISION DATE*	12/03/2020
DATA SCADENZA *EXPIRY DATE*	12/03/2023
EMISSIONE CORRENTE *CURRENT ISSUE*	12/03/2020

CERTIQUALITY S.r.l. IL PRESIDENTE
Via G. Giardino 4 – 20123 MILANO (MI) - ITALY

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SSI n. 007 G
Membro degli Accordi di Mutuo riconoscimento EA, IAF e ILAC.
Signatory of EA, IAF and ILAC Mutual Recognition Agreements.

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale.
CISQ is the Italian Federation of management system Certification Bodies.

INFORMATIVA AI SENSI DELL'ART. 13 DEL REGOLAMENTO UE 2016/679
sul trattamento dei dati personali dei soggetti che segnalano illeciti
(art. 54-bis D.Lgs. n. 165/2001)

Ai sensi e per gli effetti dell'art. 13 del Regolamento UE n. 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, in riferimento ai dati personali da Lei forniti quale segnalante (di seguito denominato "interessato"), Le vengono fornite le seguenti informazioni:

1 Titolare del trattamento (Art. 13.1.a Regolamento 679/2016/UE) **-** Il Titolare del trattamento è il **Comune di Foligno**, con sede in Piazza della Repubblica n. 10, 06034 Foligno (PG), pec: comune.foligno@postacert.umbria.it, centralino 0742/3301, il quale tratta i dati personali da Lei forniti e liberamente comunicati, garantendo che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Responsabile per la protezione dei dati personali (R.P.D.) (Art. 13.1.b Regolamento 679/2016/UE) **-** Il Titolare ha provveduto a nominare un Responsabile della protezione dei Dati Personali (R.P.D.) al quale Lei potrà rivolgersi per le questioni relative all'esercizio dei propri diritti e per richiedere informazioni sui dati personali che La riguardano che sono oggetto di trattamento da parte del Titolare.

Il R.P.D. designato dal Comune di Foligno è Anci Digitale S.p.A. la cui referente è l'Avv. Annalisa Luciani, pec: avvannalisaluciani@puntopec.it.

3. Oggetto del Trattamento - I dati personali relativi alle segnalazioni inerenti l'
acquisizione e l'archiviazione delle segnalazioni di illeciti, ai sensi dell'art. 54-bis D.Lgs. n. 165/2001, possono riguardare anche particolari categorie di dati e dati inerenti a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti agli interessati, ovvero alle persone fisiche (identificate o identificabili) che inoltrano una segnalazione o a quelle indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate.

4. Base giuridica e finalità del trattamento (Art. 13.1.c Regolamento 679/2016/UE)

I dati personali da Lei comunicati sono trattati dal Responsabile della prevenzione della corruzione e della trasparenza (RPCT) 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, ai sensi dell'art. 54-bis del D.Lgs. n. 165/2001, dai soggetti che, in ragione del proprio rapporto di lavoro presso l'Ente, vengano a conoscenza di condotte illecite, in particolare:
a) Il Segretario generale;
b) I Dirigenti, i dipendenti di ruolo e i tirocinanti;
c) I componenti dei Servizi di controllo interno;
d) I consulenti e i collaboratori;
e) I dipendenti di altre amministrazioni in posizione di comando, distacco o fuori ruolo presso l'Ente;
f) I lavoratori e i collaboratori delle imprese fornitrici di beni o servizi presso l'Ente.
Le segnalazioni possono essere effettuate nei confronti di:
a) Il Sindaco, i Consiglieri Comunali e gli Assessori dell'Ente;
b) Il Segretario generale;
c) I Dirigenti, i dipendenti di ruolo dell'Ente e i tirocinanti;
d) I componenti dei servizii di controllo interno;
e) I consulenti e i collaboratori;
f) I dipendenti di altre amministrazioni in posizione di comando, distacco o fuori ruolo presso l'Ente;
g) I lavoratori e i collaboratori delle imprese fornitrici di beni o servizi presso l'Ente, nonché altri soggetti che a vario titolo interagiscono con l'Ente stesso.
In caso di trasferimento, di comando o distacco (o situazioni analoghe) del dipendente presso altra amministrazione, questi può riferire anche di fatti accaduti in una amministrazione diversa da quella in cui presta servizio al momento della segnalazione: in tal caso la segnalazione deve essere presentata presso l'amministrazione alla quale i fatti si riferiscono ovvero all'ANAC.
Tutti i dati da Lei comunicati ,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 istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti. La gestione e la preliminare verifica sulla fondatezza delle circostanze rappresentate nella segnalazione sono affidate al RPCT che vi provvede nel rispetto dei principi di imparzialità e riservatezza effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati.

5. Modalità del trattamento
Il trattamento dei Suoi dati personali che avviene presso gli uffici del Comune di Foligno, o qualora fosse necessario, presso i soggetti indicati al paragrafo 8, è realizzato per mezzo di qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, di cui all'art. 4 n. 2) Regolamento 679/2016/UE e precisamente: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Si comunica che il trattamento dei Suoi dati personali viene compiuto con l'osservanza d'ogni misura idonea a garantirne la sicurezza e la riservatezza degli stessi.
Qualora il RPCT debba avvalersi di personale dell'Ente ai fini della gestione delle pratiche di segnalazione, tale personale per

tale attività è appositamente autorizzato al trattamento (artt. 4 n. 10, 29, 32 par. 4 Reg. UE 679/2016 e art. 2-quaterdecies D. Lgs. n. 196/2003) e, di conseguenza, il suddetto personale dovrà attenersi al rispetto delle istruzioni impartite, nonché di quelle più specifiche, connesse ai particolari trattamenti, eventualmente di volta in volta fornite dal RPCT. E' fatto salvo, in ogni caso, l'adempimento, da parte del RPCT e/o dei soggetti designati/autorizzati che per ragioni di servizio debbano conoscere l'identità del segnalante, degli obblighi di legge cui non è opponibile il diritto all'anonimato del segnalante. Con modalità tali da garantire comunque la riservatezza dell'identità del segnalante, il RPCT rende conto del numero di segnalazioni ricevute e del loro stato di avanzamento all'interno della relazione annuale di cui all'art. 1, co.14, L. n. 190/2012.
Tutti gli operatori, compreso il Titolare, per accedere ai dati informatizzati sono identificabili e dotati di password personale; l'accesso ai dati personali è consentito solo per le finalità legate al ruolo attribuito al singolo addetto, precedentemente nominato delegato al trattamento, il quale ha seguito una formazione specifica e viene periodicamente aggiornato sulle regole della privacy e sensibilizzato al rispetto e alla tutela della dignità e della riservatezza delle persone fisiche.
Il trattamento dei dati personali forniti per le finalità di cui al punto 4 viene effettuato, ai sensi dell''art. 5 del Regolamento 679/2016/UE, nel rispetto dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

6. Conferimento dei dati e conseguenze della mancata comunicazione (Art. 13.2.e Regolamento 679/2016/UE)
Tenuto conto delle finalità del trattamento come sopra illustrate, il conferimento dei Suoi personali è obbligatorio e la loro mancata, parziale o inesatta comunicazione potrà avere, come conseguenza l'impossibilità per il Titolare del trattamento di poter erogare nel modo corretto il servizio richiesto, del suo corretto svolgimento e degli eventuali adempimenti di legge.

7.Criteri utilizzati al fine di determinare il periodo di conservazione (Art. 13.2.a Regolamento 679/2016/UE)
I Suoi dati personali saranno conservati per un totale di 18 (diciotto) mesi salvo specifiche esigenze di rendicontazione annuale degli enti, che avranno avuto ampia disponibilità di tempo per la gestione ed elaborazione delle segnalazioni, avendo inoltre la piena facoltà, in completa autonomia, di esportazione parziale o totale. Decorso tale termine i dati personali saranno cancellati.

8. Ambito di diffusione, comunicazione
Qualora, all'esito della verifica, si ravvisino elementi di non manifesta infondatezza del fatto segnalato, i Suoi dati personali, unitamente all'esito dell'accertamento, potranno essere trasmessi dal RPCT per approfondimenti istruttori o per l'adozione dei provvedimenti di competenza:
a) al Dirigente del Dipartimento Risorse Umane e attività contrattuali nonché al Responsabile dell'unità organizzativa di appartenenza dell'autore della violazione, affinché sia espletato, ove ne ricorrano i presupposti, l'esercizio dell'azione disciplinare; b) agli organi e alle strutture competenti dell'Ente affinché adottino gli eventuali ulteriori provvedimenti e/o azioni ritenuti necessari, anche a tutela dell'Ente stesso;
c) se del caso, all'Autorità Giudiziaria, alla Corte dei conti e all'ANAC. In tali eventualità nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'art. 329 c.p.c.; nell'ambito l procedimento innanzi alla Corte dei Conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria; nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità.
I Suoi dati personali non verranno in alcun caso "diffusi", con tale termine intendendosi il darne conoscenza in qualunque modo ad una pluralità di soggetti indeterminati, fatti salvi gli obblighi di legge.

9. Responsabile protezione dei dati (Art. 28 Reg. UE 679/2016)
Whistleblowing Solutions Impresa Sociale s.r.l, quale fornitore del servizio di erogazione e gestione operativa della piattaforma tecnologica di digital whistleblowing, è stato nominato, dal Comune di Foligno, Responsabile del trattamento ai sensi dell'art. 28 Reg. UE n. 679/2016. Whistleblowing Solutions è il partner tecnologico selezionato da Transparency International e l'Associazione Hermes promotori del progetto Whistleblowing PA.

10. Diritti dell'interessato
In riferimento ai dati personali che La riguardano, in qualsiasi momento, ai sensi degli Artt. 15-21 del Regolamento 679/2016/UE, Lei potrà esercitare il:
• diritto di chiedere al Titolare del trattamento, ex Art. 15 Reg. 679/2016/UE, di poter accedere ai propri dati personali;
• diritto di chiedere al Titolare del trattamento, ex Art. 16 Reg. 679/2016/UE, di poter rettificare i propri dati personali, ove quest'ultimo non contrasti con la normativa vigente sulla conservazione dei dati stessi;
• diritto di chiedere al Titolare del trattamento, ex Art. 17 Reg. 679/2016/UE, di poter cancellare i propri dati personali, ove quest'ultimo non contrasti con la normativa vigente sulla conservazione dei dati stessi;
• diritto di chiedere al Titolare del trattamento, ex Art. 18 Reg. 679/2016/UE, di poter limitare il trattamento dei propri dati personali;
• diritto di opporsi al trattamento, ex Art. 21 Reg. 679/2016/UE;

11. *Diritto di presentare reclamo (Art. 13.2.d Regolamento 679/2016/UE)*
In qualità di interessato, in caso di illecito trattamento o di ritardo o impedimento da parte del Titolare all'esercizio dei Suoi diritti, Lei potrà esercitare il diritto di proporre reclamo all'Autorità di controllo.
L'Autorità di controllo competente è il Garante per la protezione dei dati personali, Piazza Venezia n. 11 – 00187 ROMA – Fax: (+39) 06.69677.3785 – Centralino telefonico: (+39) 06.696771 – E-mail: garante@gpdp.it.

12. Modalità di esercizio dei diritti
In qualità di interessato Lei potrà esercitare i propri diritti inviando una richiesta al Titolare del trattamento ai contatti sopra specificati.

Informativa aggiornata il 28/01/2023

ACCORDO IN MERITO AL TRATTAMENTO DI DATI PERSONALI

Ai sensi dell'art. 28 del Regolamento UE 2016/679

TRA

Comune di Foligno, con sede in Foligno, Piazza della Repubblica, 10, Codice Fiscale e P. IVA 00166560540 (di seguito "**Committente** " o il "**Titolare del Trattamento**") in persona di XXXXXXXXXX, nato a XXXXXXXXXXXX il XXXXXXXXXX - Segretario Generale,

E

Whistleblowing Solutions I.S. S.r.l., con sede in Viale Aretusa, 34, 20129, Milano, Codice Fiscale e P. IVA n. 09495830961, in persona di XXXXXXXXXXXXXXX (di seguito "**Fornitore** " o il "**Responsabile del Trattamento**"),

(di seguito, congiuntamente, le "**Parti**")

PREMESSO CHE

a) Le Parti hanno sottoscritto un contratto avente ad oggetto la prestazione da parte del Fornitore di un servizio di whistleblowing digitale consistente in fornitura in outsourcing di una piattaforma di whistleblowing digitale (di seguito, "**Contratto di servizi**");

b) In virtù del Contratto di servizi il Fornitore esegue operazioni di trattamento di dati personali (di seguito, "**Dati Personali**") di titolarità del Committente, e riferiti unicamente ai dati necessari per l'erogazione dei servizi pattuiti tra le parti. In particolare l'acquisizione e l'archiviazione delle segnalazioni dà luogo a trattamenti di dati personali appartenenti anche a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti agli interessati, ovvero alle persone fisiche (identificate o identificabili) che inoltrano una segnalazione o a quelle indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate (art. 4, par. 1, nn. 1) e 2), del Regolamento.

c) il Fornitore dichiara e garantisce di possedere competenza e conoscenze tecniche in relazione alle finalità e modalità di trattamento, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei Dati Personali trattati, nonché in relazione alla normativa italiana ed europea in materia di protezione dei dati personali, e di possedere i requisiti di affidabilità idonei a garantire il rispetto delle disposizioni normative in materia;

d) il Titolare ha condotto una positiva valutazione della idoneità e qualificazione del Responsabile atta a soddisfare, anche sotto il profilo della sicurezza del trattamento, i requisiti di cui alla normativa applicabile (artt. 28 e ss. del Regolamento) e intende designare il Fornitore quale Responsabile del trattamento dei Dati Personali derivante dal Contratto di servizi.

Tutto quanto sopra premesso, tenuto conto delle reciproche promesse e degli accordi intercorsi, le Parti convengono quanto segue:

1. PREMESSE

Le premesse costituiscono parte integrante ed essenziale del presente contratto.

2. OGGETTO

2.1 Con la sottoscrizione del presente contratto il Committente nomina il Fornitore, che accetta, responsabile del trattamento in relazione alle operazioni di trattamento Dati Personali poste in essere ai soli fini dell'esecuzione del Contratto di servizi. Tale nomina non comporta il diritto ad alcuna remunerazione integrativa rispetto al corrispettivo pattuito contrattualmente.
2.2 I compiti assegnati al Fornitore sono esclusivamente quelli resi necessari dalle attività connesse all'esecuzione del Contratto di servizi.

3. OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

3.1 Qualora nell'ambito delle operazioni di trattamento dei Dati Personali occorrano eventuali istruzioni aggiuntive al fine di adeguarsi alla normativa in materia di protezione dei dati, il Committente trasmetterà ulteriori istruzioni al Fornitore in merito alle finalità, modalità e procedure per l'utilizzo e il trattamento dei Dati Personali, e concorderà con il Fornitore le misure tecniche ed organizzative più idonee.

4. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

4.1 Ai fini di un corretto trattamento dei Dati Personali, il Fornitore si impegna a:

a) svolgere qualsiasi operazione di trattamento di Dati Personali in conformità ai principi e alla regolamentazione previsti dalla normativa vigente in materia di protezione dei dati personali;

b) eseguire fedelmente ed esclusivamente le istruzioni impartite dal Titolare, evitando attività di trattamento non conformi alle predette istruzioni o volte a perseguire finalità diverse da quelle correlate all'esecuzione del Contratto di servizi;

c) non effettuare copie dei Dati Personali diverse da quelle strettamente necessarie alla corretta esecuzione del Contratto di servizi;

d) garantire il pieno rispetto degli obblighi di cui il Fornitore, quale responsabile del trattamento, è tenuto in virtù della normativa vigente;

e) fuori dai casi strettamente necessari per l'erogazione dei Servizi, non divulgare o rendere noti a terzi i Dati Personali e adottare le misure organizzative e tecniche necessarie per assicurare la massima riservatezza dei Dati Personali acquisiti e utilizzati nello svolgimento delle attività oggetto della presente designazione;

f) garantire che l'accesso ai Dati Personali da parte del personale avvenga solo sulla base del principio di stretta necessità, provvedendo a individuare e designare quali incaricati del trattamento, anche ai fini di cui all'art. 32 del Regolamento Privacy, le persone fisiche (dipendenti e/o collaboratori) autorizzate al trattamento dei dati personali per le suddette finalità, impegnando gli stessi con idonei vincoli di riservatezza;

g) formare adeguatamente il personale addetto all'esecuzione del Contratto di servizi fornendo loro istruzioni precise e vigilando sulla loro osservanza;

h) collaborare con il Committente per l'attuazione di qualsiasi misura che si renda strettamente necessaria al fine di garantire la conformità del trattamento dei Dati Personali con la normativa applicabile;

i) mantenere informato il Committente riguardo alle operazioni di trattamento trasmettendo un rapporto scritto sull'attività svolta in esecuzione dei compiti attribuiti con il presente contratto, con particolare riguardo, ma non esclusivamente, alle misure di sicurezza adottate, nonché riguardo a qualsiasi circostanza o criticità eventualmente riscontrata;

j) informare il Committente, entro 48 ore dal momento in cui ne è venuto a conoscenza, di qualsiasi violazione o rischio di violazione concernente i Dati Personali di cui il Fornitore è venuto a

conoscenza nello svolgimento dei Servizi e collaborare, a proprie spese, con il Committente per attuare qualsiasi misura che si renda strettamente necessaria al fine di garantire la conformità del trattamento dei Dati Personali con la normativa applicabile;

k) adottare le misure di sicurezza previste dall'articolo 8 del presente contratto;

5. AFFIDAMENTO A TERZI

5.1 E' consentito al Fornitore di avvalersi di soggetti terzi ai fini della prestazione dei Servizi senza il preventivo consenso scritto del Titolare. Il Fornitore si impegna a prevedere nel contratto con il subappaltatore garanzie e obblighi analoghi a quelli di cui al presente contratto. il Responsabile del trattamento dichiara di avvalersi dei Subresponsabili indicati nell'Allegato A. Con la sottoscrizione del presente atto di nomina, i Subresponsabili indicati nell'Allegato A si intendono approvati dal Titolare del trattamento. Il Fornitore dichiara che i Subresponsabili hanno capacità e competenze per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni della vigente normativa sulla protezione dei dati personli e che sono stati contrattualmente vincolati al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dal Responsabile del trattamento nei confronti del Titolare. Qualora il Responsabile del trattamento intenda sostituire i Subresponsabili indicati nell'Allegato A, dovrà informare il Titolare preventivamente e per iscritto. Il Fornitore dichiara e garantisce che eventuali, nuovi, Subresponsabili presenteranno almeno le stesse caratteristiche e garanzie dei Subresponsabili indicati nell'Allegato A e saranno vincolati contrattualmente al rispetto dei medesimi obblighi in materia di protezione dei dati personali assunti dai Subresponsabili.

6. DURATA - CESSAZIONE

6.1 L'efficacia del presente contratto decorre dalla data di sottoscrizione dello stesso ad opera di entrambe le Parti sino alla cessazione, per qualsiasi causa intervenuta, del Contratto di servizi.
6.2 All'atto della cessazione del Contratto di servizi il Fornitore dovrà cessare qualsiasi operazione di trattamento dei Dati Personali e restituire al Committente tutti gli eventuali Dati Personali trattati ai fini dell'esecuzione del Contratto di servizi di cui il Fornitore dovesse disporre (es. anagrafiche degli interessati, dati di contatto degli interessati) o, su richiesta del Committente, provvedere alla loro distruzione, fornendone apposita attestazione, eccettuate eventuali esigenze di loro conservazione in adempimento di obblighi normativi di cui andrà data contestuale attestazione al Committente.

7. MISURE DI SICUREZZA

7.1 Con riferimento alle operazioni di trattamento dei Dati Personali necessarie ai fini della esecuzione del Contratto di servizi, il Fornitore dichiara e garantisce (i) di mantenere, ogni e qualsiasi misura di sicurezza idonea a prevenire i rischi di distruzione, perdita, anche accidentale, dei Dati Personali nonché di accesso non autorizzato o trattamento illecito dei medesimi come previsto nel Contratto di servizi e (ii) che tali misure sono conformi anche alle misure di sicurezza necessarie e conformi ai principi di cui all'art. 32 del Regolamento Privacy, nonché ogni altra misura obbligatoria di legge.
7.2 Con riferimento al trattamento di Dati Personali svolti con l'ausilio di strumenti elettronici per la prestazione dei Servizi e la gestione del database per conto del Committente, il Responsabile si impegna ad attuare le seguenti misure:
7.3 Il Fornitore si impegna a verificare regolarmente l'idoneità delle misure adottate.

i. scegliere gli amministratori di sistema tra quei soggetti dotati di esperienza, capacità ed affidabilità, in grado di garantire il pieno rispetto della normativa italiana in materia di protezione dei dati personali, ivi compreso il profilo relativo alla sicurezza;

ii. nominare gli amministratori di sistema individualmente, elencando analiticamente gli ambiti di operatività consentiti a ciascun amministratore di sistema in relazione al proprio profilo di autenticazione;

iii. tenere un elenco aggiornato dei soggetti nominati amministratori di sistema e, su richiesta, mettere tale elenco a disposizione del Committente e/o delle autorità competenti;

8. CONTROLLI

8.1 Il Fornitore riconosce e accetta che il Committente, nell'ambito dei poteri e obbligazioni ad esso spettanti in quanto Titolare del trattamento, possa controllare le operazioni di trattamento di Dati Personali svolte dal Fornitore, come anche le misure di sicurezza attuate da quest'ultimo per le finalità di cui al presente contratto, anche mediante appositi audit da concordarsi preventivamente nel rispetto delle reciproche esigenze lavorative.

Foligno, 6/12/2020

per Il Titolare del trattamento

XXXXXXXXXXXXXXX
(firmato digitalmente)

Whistleblowing Solutions I.S. S.r.l. preso atto di quanto previsto nel presente atto di nomina e dalla normativa vigente, dichiara di accettare l’incarico di Responsabile del trattamento.

Il Responsabile del trattamento

XXXXXXXXXXXXXXXXXXX

ALLEGATO A

(ELENCO DEGLI EVENTUALI SUBRESPONSABILI DI CUI SI AVVALE IL RESPONSABILE DEL TRATTAMENTO AL MOMENTO DELLA SOTTOSCRIZIONE DELL'ATTO DI NOMINA)

DENOMINAZIONE, SEDE E DATI DI CONTATTO DEL SUBRESPONSABILE	ATTIVITÀ DI TRATTAMENTO DEMANDATE AL SUBRESPONSABILE	LUOGO DEL TRATTAMENTO LOCALIZZAZIONE DEI SERVER
SEEWEB S.R.L	ARCHIVIAZIONE HOSTING CLOUD IASS	MILANO FROSINONE