ORDINE DEGLI AVVOCATI DI TERNI

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

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

Titolare del trattamento	Consiglio dell'Ordine degli Avvocati di Terni
Responsabile del trattamento	Whistleblowing Solutions S.r.l.
Responsabile della Protezione Dati	Avv. Piofrancesco Guida

SOMMARIO

1. Introduzione

Il 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 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 paragrafo 3 prevede che la valutazione di impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nel seguente caso: … *"b) il trattamento, su larga scala, di categorie particolari di dati personali …"*.
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; 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. 54-bis del D.Lgs. n. 165/2021 – effettuato dall'Ordine degli Avvocati di Terni.
La valutazione di impatto si riferisce alla valutazione dei rischi in cui potrebbero incorrere le libertà ed i diritti dei cittadini a causa dell'utilizzo della piattaforma informatica gratuita ed è stata svolta dal Titolare del trattamento con il supporto del Responsabile della prevenzione della corruzione e della trasparenza (RPCT).

Viene, inoltre, acquisito il parere del Responsabile della Protezione dati (DPO) – Avv. Piofrancesco Guida.
Il Titolare del trattamento provvederà: alla 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 un allegato del Registro dei trattamenti tenuto dal Consiglio dell'Ordine degli Avvocati di Terni.

2. Fonti normative

- Art. 54-bis del D.Lgs. n. 165/2001 (Testo Unico Pubblico Impiego);
- Deliberazione ANAC n. 469 del 09/06/2021;

- 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 di 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 4 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 (ad 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.

GRAVITÀ – La gravità rappresenta la 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.

PROBABILITÀ – 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, intenzionale ovvero accidentale, che comporterebbe il danno all'interessato.
VULNERABILITÀ – 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 n. 2016/679.

4. Descrizione del trattamento

Per le caratteristiche di pervasità e intrusione nella sfera dei comportamenti personali, proprie del trattamento in esame, si rende necessaria la 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. Qual è il trattamento in parola?

Il trattamento in parola è denominato WHISTLEBLOWING e scaturisce da un Contratto di servizi sottoscritto tra il Consiglio dell'Ordine degli Avvocati di Terni (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 Consiglio dell'Ordine degli Avvocati di Terni.
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 Consiglio dell'Ordine degli Avvocati di Terni, in qualità di Titolare del trattamento, ha designato per il trattamento dei dati personali i propri dipendenti, ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003 e, quanto alle funzioni in materia di anticorruzione e trasparenza, l'Avv. Marco Proietti quale Responsabile della prevenzione della corruzione e per la trasparenza (RPCT), il quale svolge tale attività nella 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 della integrità dell'Ente.

3. Ci sono standard applicabili al trattamento?

Per gli standard applicabili al trattamento si rinvia a quelli previsti dalla normativa in materia di privacy.

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 Presidente e i Consiglieri dell'Ente;
- 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 del 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.

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, co. 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 Consiglio dell'Ordine degli Avvocati di Terni tutti gli eventuali dati personali di cui dovesse disporre (ad es., anagrafiche degli interessati, dati di contatto degli interessati) ovvero, 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 Consiglio stesso.

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. Qual 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 la 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 la 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 la adozione dei provvedimenti di competenza:

a) al Dirigente responsabile del Servizio Risorse Umane e/o al Responsabile della Area organizzativa di appartenenza dell'autore della violazione, affinché sia espletato, ove ne ricorrano i presupposti, l'esercizio della 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, la identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 c.p.p.; nell'ambito del procedimento davanti alla Corte dei Conti, la identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria; nell'ambito del procedimento disciplinare la 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 e, 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 invio della richiesta, via e-mail, all'indirizzo consiglio@ordineavvocati.terni.it o all'indirizzo PEO del Responsabile della Protezione dei dati – DPO avvocato@piofrancescoguida.it.

3. Quali sono le risorse di supporto dei dati?

Le risorse impiegate per il trattamento in esame comprendono:

- connessione 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);
- firewall (uno per ogni connessione internet SPC).

6. Principi fondamentali

A) PROPORZIONALITÀ E NECESSITÀ
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.

Gli scopi perseguiti con il trattamento denominato Wistleblowing risultano, in termini generali, leciti, ai sensi dell'art. 5, para. 1, lett. a) del Reg. UE n. 2016/679.

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

La base legale, che rende lecito il trattamento, è la:

- sua necessità per la esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, di cui è investito il Titolare del trattamento (art. 6, para. 1. lett. e) del Reg. UE n. 2016/679).

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, para. 1, lett. c) del Reg. UE 679/2016, cioè 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, para. 1, lett. d) del Reg. UE n. 2016/679, i dati trattati sono esatti e, se necessario, aggiornati.
Inoltre, il Consiglio dell'Ordine degli Avvocati di Terni adotta tutte le misure ragionevoli per cancellare o rettificare, tempestivamente, i dati inesatti rispetto alle finalità per le quali sono trattati.

5. Qual 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, para. 1, lett. e) del Reg. UE n. 2016/679.
Come detto, il Responsabile del trattamento all'atto della cessazione del Contratto dovrà restituire al Consiglio dell'Ordine degli Avvocati di Terni 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 esso fornirà contestuale attestazione al Consiglio dell'Ordine degli Avvocati di Terni.
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?

La informativa resa ai soggetti interessati, ai sensi dell'art. 13 del Reg. UE n. 2016/679, è pubblicata sul sito web dell'Ordine degli Avvocati di Terni – Tool WhistleblowingPA.

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 del Reg. UE n. 2016/679 mediante il deposito di specifica istanza. Ai sensi dell'art. 20, para 3 del Reg. UE n. 2016/679, 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 n. 2016/679, mediante deposito di specifica istanza.
L'esercizio del diritto di cancellazione (cd. diritto all'oblio), ai sensi dell'art. 17, para 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 (RPCT).

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 06/10/2023, che si allega alla presente Valutazione di Impatto.

7. In caso di trasferimento di dati al di fuori della 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:

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

- **TRACCIABILITÀ**: 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 dell'Ordine 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:

- **VULNERABILITÀ**: la rete dell'Ordine 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. Il server è fisicamente in una stanza chiusa e le chiavi sono in possesso solo dei dipendenti dei servizi informatici.
- **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.
- **BACKUP**: politiche di Backup sicuri e protetti giornalieri, settimanali e mensili, anche in siti diversi.
- **MANUTENZIONE**: manutenzione dei PC, manutenzione eseguita anche da remoto ed in maniera automatica.
- **CONTRATTO CON IL RESPONSABILE DEL TRATTAMENTO**: Il Consiglio dell'Ordine degli Avvocati di Terni 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 n. 2016/679; inoltre, il Responsabile del Trattamento dati (Whistleblowing Solutions I.S. S.r.l) ha sottoscritto, con Associazione Transparency International Italia, un Accordo di collaborazione.
- **SICUREZZA DEI CANALI INFORMATICI**: Il Consiglio dell'Ordine degli Avvocati di Terni, 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 Consiglio dell'Ordine degli Avvocati di Terni ha provveduto:
  - alla designazione del Responsabile della Protezione Dati (DPO), ai sensi dell'art. 37 Reg. Ue n. 2016/679;

- alla designazione e delega dei soggetti di cui all'art. 2-quaterdecies del D.Lgs. n. 196/2003 ai fini della nomina degli Incaricati 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 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 anche significativi, ma superabili malgrado delle 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 (ad 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 anche significativi, ma superabili malgrado delle 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 (ad 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, 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 si dovesse concretizzare?

Qualora il rischio si dovesse concretizzare, gli interessati potrebbero sperimentare IMPATTI LIMITATI ovvero inconvenienti anche significativi, ma superabili malgrado delle 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 (ad 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, 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

9. Parere del RPD / DPO

A seguito di attenta analisi del presente documento, visto l'art. 39, para. 1, lett. c) del Reg. UE n. 2016/679, il sottoscritto Avv. Piofrancesco Guida, in qualità di DPO designato, tenuto conto:

- della 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 parola, 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 n. 2016/679.
Per tale ragione, non si ritiene necessario procedere con la Consultazione preventiva ex art. 36 del Reg. UE n. 2016/679.
Il presente documento viene sottoscritto digitalmente dal DPO Avv. Piofrancesco Guida.

* * * * *

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 I.S. S.r.l.;
3. Certificazione ISO/IEC 27001:2017;
4. Informativa ai sensi dell'art. 13 del Reg. UE n. 2016/679;
5. Accordo in merito al trattamento dei dati personali tra Consiglio dell'Ordine degli Avvocati di Terni e Whistleblowing Solutions I.S. S.r.l. (Nomina Responsabile del trattamento);
6. Documentazione a supporto del Titolare per la DPIA.

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: XXXXXXXXXXXXXXXXXXX

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

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.

WHISTLEBLOWING SOLUTIONS IMPRESA SOCIALE S.r.l.

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.

ORDINE DEGLI AVVOCATI DI TERNI

Informativa sul trattamento dei dati personali ai sensi dell'art. 13 del Regolamento (UE) 2016/679

Ai sensi dell'art. 13 del Regolamento (UE) 2016/679 (di seguito GDPR), recante disposizioni a tutela delle persone fisiche rispetto al trattamento dei dati personali, e del D. Lgs. 30 giugno 2003, n. 196 (Codice Privacy), La informiamo che i dati personali che ci verranno da Lei forniti con la presentazione di una segnalazione effettuata ai sensi e per gli effetti di cui al d.lgs. 10 marzo 2023, n. 24 saranno oggetto di trattamento da parte dell'Ordine degli Avvocati di Terni e Le forniamo le seguenti informazioni.

1. **Titolare del trattamento**

Il Titolare del trattamento è il Consiglio dell'Ordine degli Avvocati di Terni (Codice Fiscale: 80006130555 - Partita IVA: 01467490551), in persona del Presidente e legale rappresentante pro tempore, con sede in Via Cesare Bazzani n. 18 – 05100 Terni.

2. **Responsabile della protezione dei dati (DPO)**

Il Responsabile della protezione dei dati (DPO/RPD) è l'Avv. Piofrancesco Guida, nominato con Delibera del Consiglio dell'Ordine degli Avvocati di Terni del 14.04.2022, contattabile al seguente indirizzo di posta elettronica certificata piofrancesco.guida@ordineavvocatiterni.it;

3. **Finalità del trattamento e base giuridica**

I dati personali che ci verranno da Lei forniti con la presentazione di una segnalazione effettuata ai sensi e per gli effetti di cui al d.lgs. 10 marzo 2023, n. 24 saranno trattati dall'Ordine degli Avvocati di Terni per le esclusive finalità istituzionali conseguenti al rispetto di tale normativa. Tali attività sono disciplinate dal "Regolamento in materia di protezione delle persone che segnalano violazioni del diritto nazionale e dell'Unione europea" adottato con Delibera del Consiglio dell'Ordine degli Avvocati di Terni del 18.09.2023, pubblicato sul sito istituzionale dell'Ordine degli Avvocati di Terni alla pagina "Whistleblowing", che La invitiamo a leggere con attenzione. Nello svolgimento delle attività di cui sopra, l'Ordine potrebbe trovarsi a raccogliere e a trattare sia dati personali comuni sia dati personali qualificabili come "categorie particolari di dati personali", e cioè quei dati che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi allo stato di salute o alla vita sessuale o all'orientamento sessuale della persona", sia, infine, "dati personali relativi

a condanne penali e ai reati o a connesse misure di sicurezza". Le basi giuridiche del trattamento sono le seguenti:
- quanto ai dati personali comuni, art. 6, paragrafo 1, lettera e) del GDPR, in quanto il trattamento è 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;
- quanto ai dati personali rientranti in categorie particolari, art. 9, paragrafo 2, lettera g) del GDPR, in quanto il trattamento è necessario per motivi di interesse pubblico rilevante.

4. **Modalità di trattamento e conservazione**

Il trattamento sarà effettuato dall'Ordine degli Avvocati di Terni con modalità informatiche e cartacee, nel rispetto di quanto previsto dall'art. 32 del GDPR in materia di misure di sicurezza, ad opera di soggetti appositamente designati, autorizzati, formati e dotati di apposite istruzioni ex art. 29 del GDPR e da responsabili del trattamento appositamente designati in conformità all'art. 28 del GDPR, così come meglio specificato nel summenzionato "Regolamento in materia di protezione delle persone che segnalano violazioni del diritto nazionale e dell'Unione europea" . Nel rispetto dei principi di liceità, limitazione delle finalità e minimizzazione dei dati, di cui all'art. 5 del GDPR, i dati personali raccolti a seguito del ricevimento di segnalazioni effettuate ai sensi e per gli effetti del d.lgs. 10 marzo 2023, n. 24 e della gestione delle segnalazioni ricevute saranno trattati per il periodo di tempo necessario per la gestione delle segnalazioni ricevute e, comunque, non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

5. **Ambito di diffusione e comunicazione e categorie dei destinatari**

La informiamo che i dati personali raccolti e trattati dall'Ordine degli Avvocati di Terni nell'ambito delle procedure di segnalazione di cui al d.lgs. 10 marzo 2023, n. 24 saranno oggetto di comunicazione, esclusivamente per le finalità e nei limiti di cui al precedente articolo 3, all'Autorità giudiziaria o altre Autorità pubbliche in adempimento degli obblighi di legge ai quali l'Ordine è soggetto.

6. **Trasferimento dei dati personali**

I Suoi dati personali non saranno trasferiti né in Stati membri dell'Unione Europea né in Paesi terzi non appartenenti all'Unione Europea e/o ad organizzazioni internazionali, fatti salvi eventuali obblighi di legge ai quali l'Ordine è soggetto.

7. **Esistenza di un processo decisionale automatizzato**

L'Ordine degli Avvocati di Terni non adotta alcun processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, del GDPR.

8. **Diritti dell'interessato**

I diritti riconosciuti all'interessato, di cui agli articoli da 15 a 22 del GDPR, potranno essere esercitati nei limiti di quanto previsto dall'art. 2-undecies del d.lgs. 30 giugno 2003, n. 196, con richiesta scritta da inviarsi al Responsabile della prevenzione della corruzione e della trasparenza dell'Ordine degli Avvocati di Terni Avv. Marco Proietti in modalità alternativa: a) a mezzo posta ordinaria, all'indirizzo di cui al precedente articolo 1, in busta chiusa recante la dicitura "Riservata personale – segnalazione whistleblowing"; b) all'indirizzo di posta elettronica certificata: ord.terni@cert.legalmail.it .
Terni, data 18.09.2023

Ordine degli Avvocati di Terni
Il Presidente
Avv. Andrea Colacci

Il Presidente Avv. Andrea Colacci

ACCORDO IN MERITO AL TRATTAMENTO DI DATI PERSONALI

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

Documento aggiornato il 15 luglio 2023

TRA

CONSIGLIO DELL'ORDINE DEGLI AVVOCATI DI TERNI

con sede in TERNI, VIA CESARE BAZZANI N. 18

Codice Fiscale e P. IVA n. 80006130555

in persona di PRESIDENTE DELL'ORDINE DEGLI AVVOCATI DI TERNI

(di seguito "**Committente** " o il "**Titolare del Trattamento**"),

E

Whistleblowing Solutions I.S. S.r.l., con sede in Viale Abruzzi 13/A, 20131, Milano, Codice Fiscale e P. IVA 09495830961 del legale rappresentante pro tempore [redacted]

(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 o che rivelino, tra l'altro, l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche e l'appartenenza sindacale, 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 accordo.

2. OGGETTO

2.1 Con la sottoscrizione del presente accordo 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.

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) effettuare, ai sensi dell'art. 32 del Regolamento UE 2016/679, regolari analisi dei rischi per adottare misure tecniche organizzative adeguate rispetto alle prescrizioni di legge in materia di protezione dei dati personali, di informatica giuridica e amministrazione digitale di cui al CAD e disciplina applicabile, nonché dei provvedimenti del Garante per la protezione dei dati personali e dell'Agenzia per l'Italia Digitale (AGID) o altra Autorità di controllo competente;
j) stabilire, nell'ambito della propria organizzazione, i c.d. mezzi non essenziali, quali misure di sicurezza di dettaglio, e sulla base delle proprie competenze tecniche specifiche, collaborare, anche manifestando un'autonomia propositiva, nell'adozione di misure adeguate e nella verifica sistematica dell'efficacia delle stesse tramite una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento;
k) effettuare analisi che esplicitino i rischi e le eventuali possibili misure di attenuazione degli stessi da proporre al Titolare, propedeutiche a valutazioni di impatto, informando quest'ultimo e fornendo copia degli elaborati finali.
l) mantenere informato il Committente riguardo alle operazioni di trattamento trasmettendo un rapporto scritto sull'attività svolta in esecuzione dei compiti attribuiti con il presente accordo, con particolare riguardo, ma non

esclusivamente, alle misure di sicurezza adottate, nonché riguardo a qualsiasi circostanza o criticità eventualmente riscontrata;

m) 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;

n) adottare le misure di sicurezza previste dall'articolo 7 del presente accordo.

5. AFFIDAMENTO A TERZI

5.1 È 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 accordo. 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 personali 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, con un preavviso di 60 giorni. Resta ferma la possibilità di derogare al termine di preavviso, nel caso siano necessarie operazioni di mitigazione di un disastro imputabile al subfornitore. 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 accordo 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:

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;

7.3 Il Fornitore si impegna a verificare regolarmente l'idoneità delle misure adottate.

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 accordo, anche mediante appositi audit da concordarsi preventivamente nel rispetto delle reciproche esigenze lavorative.

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.

Luogo e data TERNI, LI 6 OTTOBRE 2023

_____	_____
Il Titolare del trattamento	Il Responsabile del trattamento Whistleblowing Solutions Impresa Sociale S.r.l. Legale Rappresentante [redacted]

ALLEGATO A

Elenco dei 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
SEEWEB S.R.L	ARCHIVIAZIONE HOSTING CLOUD IASS	MILANO FROSINONE (BACKUP)
TRANSPARENCY INTERNATIONAL ITALIA	SUPPORTO UTENTI AMMINISTRATORE DI SISTEMA	MILANO

WHISTLEBLOWINGIT

DOCUMENTAZIONE A SUPPORTO DEL TITOLARE PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

TRATTAMENTO DATI RELATIVI ALLE SEGNALAZIONI DI CONDOTTE ILLECITE (C.D. WHISTLEBLOWING)

Documento aggiornato il 15 luglio 2023

WHISTLEBLOWINGIT
Un progetto di Whistleblowing Solutions Impresa Sociale e Transparency International Italia
www.whistleblowing.it | info@whistleblowing.it

WHISTLEBLOWINGIT

SOMMARIO

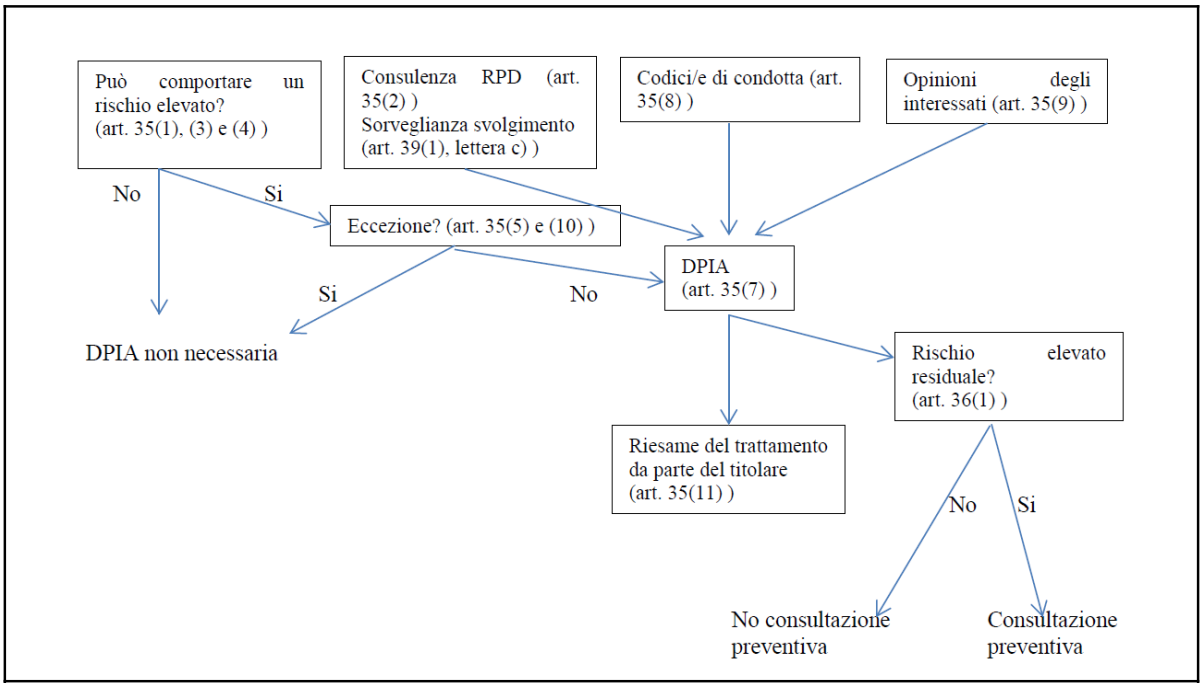
1. PREMESSA

La Valutazione d'Impatto sulla Protezione dei Dati (di seguito "DPIA) è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del titolare nei confronti dei trattamenti dallo stesso effettuati.

Il Titolare del trattamento, infatti, è tenuto non solo a garantire l'osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

Whistleblowing Solutions, nel suo ruolo di Responsabile del trattamento per la gestione del sistema di whistleblowing, con il presente documento intende fornire tutti gli elementi ai Titolari per svolgere la valutazione di impatto così come previsto dall'art. 35 del Regolamento.



Principi fondanti il processo di DPIA

2. DESCRIZIONE DELLA PIATTAFORMA DI WHISTLEBLOWING

Whistleblowing Solutions, in qualità di responsabile del trattamento, si occupa della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.

ARCHITETTURA DI SISTEMA

L'architettura di sistema è principalmente composta da:

- Un cluster di due firewall perimetrali;
- Un cluster di due server fisici dedicati;
- Una Storage Area Network pienamente ridondata.

SOFTWARE IMPIEGATO

La piattaforma informatica di segnalazione è basata sul software libero ed open-source **GlobaLeaks** di cui Whistleblowing Solutions è co-autore e coordinatore di progetto.

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.

Vengono primariamente utilizzati le tecnologie open source:

- Debian/Linux (principale sistema operativo utilizzato);
- Postfix (mail server);
- Bind9 (dns server);
- OPNSense (firewall);
- OpenVPN (vpn).

Le limitate componenti software di natura proprietaria impiegate sono le seguenti:

- VMware, software di virtualizzazione;
- Veeam, software di backup;
- Plesk, software per realizzazione siti web di facciata del progetto.

Predisposizione dei sistemi virtualizzati:

- 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.

ARCHITETTURA DI RETE

- L'architettura di rete prevede un firewall perimetrale e segregazione della rete in molteplici VLAN al fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente;
- Una VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definito insieme di amministratori di sistema;
- Ogni connessione di rete implementa TLS 1.2+;
- Ogni macchina virtuale istanziata vede esposizione di rete limitata all'effettiva necessità;
- Tutti i dispositivi utilizzati quali l'applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log e/o informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP e User Agents;
- L'applicativo GlobaLeaks abilita la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

3. DESCRIZIONE E ANALISI DEL CONTESTO

Responsabilità connesse al trattamento:	**PA, Ente o Organizzazione** > Titolare del trattamento **Whistleblowing Solutions** > Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing **Seeweb** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS) **Transaparency International Italia** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing **Conformità normativa:**
Standard applicabili:	• ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks" • ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud • ISO27018 per la protezione dei dati personali nei servizi Public Cloud • Qualifica AGID • Certificazione CSA Star
Dati e operazioni di trattamento:	Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti. **Dati di registrazione** Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione). **Categorie particolari di dati** Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati. **Dati relativi a condanne penali e reati** Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Ciclo di vita del trattamento e dei dati	1) Attivazione della piattaforma 2) Configurazione della piattaforma 3) Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti 4) Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore
Risorse a supporto delle attività di trattamento:	Software di whistleblowing professionale GlobaLeaks Infrastruttura IaaS e SaaS privata basata su tecnologie: - Dettaglio Hardware - VMWARE (virtualizzazione) - Debian Linux LTS (sistema operativo) - VEEAM (backup) - OPNSENSE (firewall) - OPENVPN (vpn)

4. VALUTAZIONI IN MERITO AI TRATTAMENTI

PRINCIPI FONDAMENTALI

Adeguatezza, pertinenza e limitazione a quanto è necessario in relazione alle finalità per le quali i dati sono trattati (minimizzazione)	Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI). Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia. Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

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

Periodo di conservazione dei dati	Policy di data retention di default delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte.

	Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.

Definizione degli obblighi dei responsabili del trattamento e formalizzazione dei contratti	Gli accordi contrattuali sono definiti con le seguenti società: • Whistleblowing Solutions in qualità di Responsabile del trattamento • Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions • Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions

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

5. MISURE DI SICUREZZA

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 sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.

Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

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.

Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

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.

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

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.

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 crescente 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.

Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html

BACKUP

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

MANUTENZIONE

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

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

Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

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.

SICUREZZA DELL'HARDWARE

I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7×24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7×24.

I datacenter del fornitore IaaS sono certificati ISO27001.

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.

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.

6. MISURE ADDIZIONALI

Il presente documento sintetizza una serie di metodologie standard conformi con la normativa vigente in ambito nazionale ed internazionale in materia di trattamento sicuro dell'informazione, privacy e whistleblowing.

A queste si aggiunge un crescente insieme altre misure al passo con la ricerca e la tecnica in ambito di sicurezza informatica reperibile alle seguenti pagine web:

- THREAT MODEL
- APPLICATION SECURITY