PROVINCIA DI TERNI

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

SISTEMA DI SEGNALAZIONE

"WHISTLEBLOWING"

(art. 54bis D.Lgg. 165/2001)

Titolare del trattamento	Provincia di Terni
Responsabile del trattamento	Whistleblowing Solutions IS s.r.l.
Responsabile Protezione Dati	Unica Soc. Coop. - referente RPD Dott. Giuliano Palotto

SOMMARIO

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".*

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;

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 dalla Provincia di Terni.

Per le caratteristiche di pervasività e possibile intrusione nella sfera dei comportamenti personali, proprie del trattamento in esame, si rende necessaria l'effettuazione della presente valutazione di impatto del trattamento.

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 individuata (Whistleblowing Solutions I.S. S.r.l.) 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), del DPO Dott. Giuliano Palotto e del Responsabile del Servizio Procedure informatiche centrali, supporto per il digitale e statistica, Dott. Paolo Onori.

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 viene pubblicata sul sito web della Provincia di Terni, 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 (Linee Guida in materia di whistleblowing, in attesa delle nuove Linee Guida, in consultazione);
- D.Lgs. 24/2023 di recepimento della Direttiva UE 2019/1937;
- 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

Il trattamento in considerazione è denominato WHISTLEBLOWING e scaturisce da un Contratto di servizi sottoscritto tra la Provincia 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 o di collaborazione 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.
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.

5. Contesto

1. 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 della Provincia 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, nonché, sempre in qualità di sub-responsabile, di Trasparency International Italia.
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, in base a quanto previsto dalla vigente normativa, con particolare riferimento, da ultimo, alle disposizioni del D.Lgs. 24/2023 attuativo della 1937/2019.

La Provincia di Terni, in qualità di Titolare del trattamento, con Decreto del Presidente n. 6976 del 17/5/2023, 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.
Qualora il RPCT debba avvalersi di personale dell'Ente ai fini della gestione delle pratiche di segnalazione, il personale per tale attività sarà 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.
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.

2. **Ci sono standard applicabili al trattamento?**

Per gli standard applicabili al trattamento si rinvia all'Art. 6 del vigente Codice di comportamento integrativo della Provincia di Terni, pubblicato sul sito web dell'Ente.

6. 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 della Provincia di Terni - Sezione Amministrazione Trasparente – Altri contenuti – Prevenzione e corruzione – Whistleblowing Segnalazioni condotte illecite (Allegato 6 alla presente DPIA)

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, tramite PEC indirizzata al titolare Amministrazione Provinciale di Terni all'indirizzo provincia.terni@postacert.umbria.it o all'indirizzo mail del Responsabile della Protezione dei dati – DPO dpo@provincia.terni.it .
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, tramite PEC indirizzata al titolare Amministrazione Provinciale di Terni all'indirizzo provincia.terni@postacert.umbria.it o all'indirizzo mail del Responsabile della Protezione dei dati – DPO dpo@provincia.terni.it.
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, tramite mail segretario@provincia.terni.it .

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 con la Provincia di Terni che si allega alla presente Valutazione di Impatto (Allegato 2 alla presente DPIA).

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.

Per ogni altro aspetto connesso alla valutazione dei rischi per i diritti e le libertà degli interessati, nonché alle 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 alle vigenti normative, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione, si fa espresso rinvio **all'allegato 1 alla presente DPIA (DOCUMENTAZIONE A SUPPORTO DEL TITOLARE PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI ELABORATA DA WHISTLEBLOWING SOLUTIONS IS SRL).**

7. Rischi

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

La gravità del rischio stimata è: LIMITATA

2. 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. Allegati

1. DOCUMENTAZIONE A SUPPORTO DEL TITOLARE PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI ELABORATA DA WHISTLEBLOWING SOLUTIONS IS SRL
2. NOMINA RESPONSABILE DEL TRATTAMENTO (ACCORDO PROVINCIA DI TERNI / WHISTLEBLOWING SOLUTIONS IS SRL)
3. NOMINA SUB-RESPONSABILI DEL TRATTAMENTO (ACCORDI WHISTLEBLOWING SOLUTIONS IS SRL / TRASPARENCY INTERNATIONAL ITALIA E WHISTLEBLOWING SOLUTIONS IS SRL / SEEWEB S.R.L.)
4. CERTIFICAZIONE ISO/IEC 27001:2017 DI WHISTLEBLOWING SOLUTIONS IS SRL
5. CONFORMITÀ AL PRINCIPIO DNSH DO NOT SIGNIFICATIVE HARM DI WHISTLEBLOWING SOLUTIONS IS SRL
6. INFORMATIVA AI SENSI DEGLI ARTT. 13 E 14 REG. UE 2016/679

9. Parere degli interessati

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

10. <u>Parere del R.P.D./D.P.O.</u>

A seguito di attenta analisi del presente documento, visto l'art. 39 par. 1 lett. C) del Reg. UE 2016/679, il Dott. Giuliano Palotto, in qualità di referente del D.P.O. designato da Unica Soc. Coop. a r.l., 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 <u>medio-bassi</u>.
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, ciascuno per quanto di competenza, dal RPCT Dott. Paolo Ricciarelli e dal DPO Dott. Giuliano Palotto.

Firmato digitalmente da:
Ricciarelli Paolo
Firmato il 29/06/2023 09:29
Seriale Certificato: 1628472
Valido dal 15/07/2022 al 15/07/2025
InfoCamere Qualified Electronic Signature CA

Firmato digitalmente da:
PALOTTO GIULIANO
Firmato il 29/06/2023 09:49
Seriale Certificato: 1805042
Valido dal 05/10/2022 al 05/10/2025
InfoCamere Qualified Electronic Signature CA

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 11 gennaio 2023

SOMMARIO

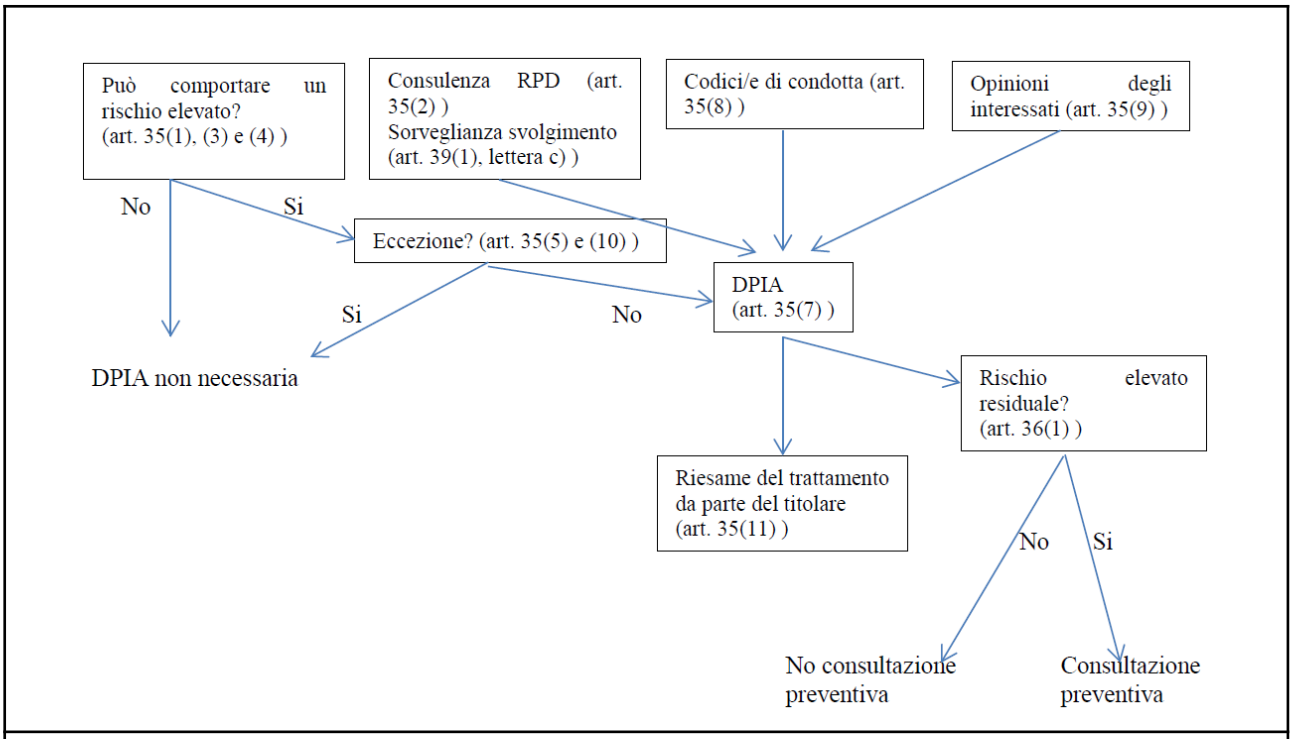
1. PREMESSA

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 18 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.

Definizione degli obblighi dei responsabili del trattamento e	Gli accordi contrattuali sono definiti con le seguenti società:

formalizzazione dei contratti	• 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

ACCORDO IN MERITO AL TRATTAMENTO DI DATI PERSONALI

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

Documento aggiornato il 6 aprile 2023

TRA

PROVINCIA DI TERNI

con sede in VIALE DELLA STAZIONE, 1

Codice Fiscale e P. IVA n. 00179350558

in persona di PAOLO RICCIARELLI

(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 Ing. Giovanni Pellerano (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 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.

Terni, 5-6-2023

Luogo, Data

RICCIARELLI
PAOLO
05.06.2023
15:09:49
UTC

Il Titolare del trattamento

Giovanni Pellerano

Il Responsabile del trattamento
Whistleblowing Solutions Impresa Sociale S.r.l.
Legale Rappresentante
Giovanni Pellerano

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

ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI

AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679

("REGOLAMENTO")

TRA

Whistleblowing Solutions Impresa Sociale S.r.l.

(Responsabile del Trattamento)

E

Transparency International Italia

(Sub-Responsabile del Trattamento)

In relazione all'accordo per il supporto alla gestione delle piattaforme di whistleblowing

1. Premessa

1.1. Premesso che:

A. Il presente Accordo prevede che il Trattamento di Dati Personali che **Whistleblowing Solutions Impresa Sociale S.r.l.** ("**WBS**") effettua quale Responsabile del trattamento per conto dei propri Clienti, Titolari del trattamento.

B. Transparency International Italia ("**TRANSPARENCY**") dichiara di avere tutte le competenze tecniche e organizzative idonee, ai sensi e per gli effetti dell'art. 28 del Regolamento, al ruolo di Sub-Responsabile del Trattamento dei Dati Personali per l'esecuzione dell'Accordo di cui il presente documento costituisce un allegato.

C. WBS e TRANSPARENCY si danno reciprocamente atto che:

a) WBS è Responsabile del Trattamento dei Dati dei propri Clienti, Titolari del Trattamento;
b) TRANSPARENCY è Sub-Responsabile dei Dati Personali Trattati in esecuzione del Servizio oggetto del Contratto; in particolare, pertanto, i compiti e le responsabilità di TRANSPARENCY sono strettamente legati al diretto adempimento delle obbligazioni assunte nell'ambito del Contratto, con esclusione di ogni altra responsabilità.
c) il presente accordo e le sue appendici (congiuntamente denominati "Accordo per il Trattamento dei Dati Personali" o anche "Accordo TDP"), sono sottoscritti da WBS e TRANSPARENCY al fine di dettagliare le istruzioni e regolare il rapporto tra il Responsabile e il Sub-Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento, anche con riferimento ai rispettivi diritti e obblighi relativi al Trattamento dei Dati Personali ed in particolare per stabilire misure di sicurezza e procedure idonee per procedere al legittimo Trattamento dei Dati Personali; il presente Accordo TDP è a titolo gratuito in quanto collegato alla fornitura del Servizio;
d) con il presente Accordo TDP, WBS affida a TRANSPARENCY tutte ed esclusivamente le operazioni di Trattamento dei Dati Personali necessarie per dare piena esecuzione al Servizio, come descritto nel Contratto e nei suoi allegati.

D. In particolare, la finalità perseguita, la tipologia, e le modalità del Trattamento dei Dati Personali sono descritti nell'**Appendice 1.**

E. In caso di contrasto o incongruenze per quanto riguarda gli accordi tra le Parti in materia di protezione dei Dati Personali tra il presente Accordo TDP e il Contratto, prevale quanto stabilito nell'Accordo TDP ed in eventuali accordi integrativi o modificativi di quest'ultimo.

F. La presente premessa forma parte integrante dell'Accordo TDP.

2. Definizioni

2.1. Salvo che sia diversamente definito nel presente Accordo TDP, tutti i termini utilizzati nel presente documento e nelle sue appendici hanno il significato loro attribuito nel Contratto.

"**Accordo per il Trattamento dei Dati Personali" o "Accordo TDP**" indica il presente accordo per il Trattamento dei Dati Personali comprensivo delle Appendici 1, 2 e 3, nonché di eventuali accordi modificativi o integrativi;

"**Autorità di Controllo**" indica ogni autorità competente a vigilare ed assicurare l'applicazione delle Leggi applicabili in materia di protezione dei Dati Personali con riferimento al Trattamento dei Dati Personali svolti per mezzo del Servizio;

"Categorie Particolari di Dati Personali" indica i Dati Personali che rivelino: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il Trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

"**Contratto**" indica **l'accordo per il supporto alla gestione delle piattaforme di whistleblowing**.

"Dati Giudiziari" indicano i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;

"Dati Personali" significa qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; al fine di evitare contrasti interpretativi, ha in ogni caso il significato previsto dal Regolamento e dalle Leggi applicabili in materia di protezione dei Dati Personali;

"Diritti dell'Interessato" sono i diritti riconosciuti all'Interessato dalle Leggi applicabili in materia di protezione dei Dati Personali come, nei limiti di applicabilità del Regolamento, ad esempio, il diritto di chiedere l'accesso, la rettifica o la cancellazione dei Dati Personali, il diritto alla limitazione del Trattamento dei dati dell'Interessato o il diritto di opposizione al Trattamento, nonché il diritto alla portabilità dei dati;

"**Elenco dei Sub-Responsabili**" indica l'elenco disponibile nell'**Appendice 3**;

"Incaricato/i" il personale, dipendenti, collaboratori a qualsiasi titolo del Prestatore che abbiano accesso ai Dati Personali e agiscono ai sensi dell'art. 29 del Regolamento;

"Interessato/i" ha il significato previsto dal Regolamento;

"Leggi applicabili in materia di protezione dei Dati Personali" indica, negli Stati membri dell'Unione Europea, il Regolamento e le complementari legislazioni nazionali in materia di

protezione dei Dati Personali, comprensivi di ogni orientamento e/o *code of pratice* emessi dalla competente Autorità di Controllo all'interno dell'Unione Europea (inclusi i provvedimenti e/o delle Autorizzazioni e/o Linee Guida del Garante per la protezione dei dati personali in quanto applicabili); e/o, negli Stati extra UE, ogni vigente legislazione in materia di protezione dei Dati Personali relativa alla tutela ed al legittimo Trattamento di Dati Personali;
"Regolamento" indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE;
"Responsabile del Trattamento" indica la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che effettua un Trattamento dei Dati Personali per conto del Titolare;
"**Servizio**" indica il servizio oggetto del Contratto di cui il presente Accordo TDP costituisce allegato;
"**Sub-Responsabile**" indica un organismo individuato dal Responsabile per assisterlo nel Trattamento dei Dati Personali del Titolare;
"Titolare" indica la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che, da solo o congiuntamente con altri soggetti, determini le finalità e le modalità del Trattamento dei Dati Personali relativi alle segnalazioni di condotte illecite (c.d. whistleblowing);
"Trattare" o "**Trattamento**" significa qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come 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;
"**UE**" indica l'Unione Europea;
"Violazione dei Dati Personali" indica la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

3. Obblighi del Sub-Responsabile del trattamento

3.1. TRANSPARENCY, per quanto di competenza, è tenuto, in forza di legge e di contratto, per sé e per gli Incaricati e per qualunque soggetto collabori con la sua attività, al rispetto delle Leggi applicabili in materia di protezione dei Dati Personali.
3.2. Fatti salvi gli obblighi stabiliti da altre disposizioni del presente Accordo TDP, TRANSPARENCY del Trattamento è obbligato a:

a) trattare i Dati Personali solo per quanto strettamente necessario all'erogazione del Servizio e solo limitatamente alla conduzione tecnico funzionale dei sistemi/servizi oggetto del Contratto;
b) rispettare le istruzioni impartite da WBS per iscritto con il presente Accordo TDP e con eventuali accordi scritti successivi, avvertendo WBS qualora ritenga che le istruzioni impartite si pongano in violazione delle Leggi applicabili in materia di protezione dei Dati Personali;
c) contestualmente alla designazione, fornire adeguate istruzioni scritte agli Incaricati circa le modalità del Trattamento dei Dati Personali in ottemperanza a quanto disposto dalle Leggi applicabili in materia di protezione dei Dati Personale e dal presente Accordo TDP. A titolo esemplificativo e non esaustivo, TRANSPARENCY, nel designare per iscritto gli Incaricati, dovrà prescrivere che essi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Inoltre per i Trattamenti effettuati per fornire il Servizio dagli Incaricati con mansioni di "Amministratore di Sistema", TRANSPARENCY è tenuta altresì al rispetto del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (modificato in base al provvedimento del 25 giugno 2009) e delle Leggi applicabili in materia di protezione dei Dati Personali pro tempore applicabili relative alla disciplina sugli amministratori di sistema. La versione aggiornata dell'elenco contenente gli estremi identificativi (nome, cognome, funzione o area organizzativa di appartenenza) degli Amministratori di Sistema dovrà essere consegnato senza indugio a semplice richiesta anche solo verbale di WBS, a quest'ultimo e/o alle competenti Autorità e ad eventuali ulteriori terzi aventi diritto;
d) vincolare gli Incaricati alla riservatezza, anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto, in relazione alle operazioni di Trattamento da essi eseguite;
e) verificare che gli Incaricati di cui al punto precedente applichino tutte le disposizioni in materia di sicurezza adottate ai sensi dell'art. 32 del Regolamento (per quanto di loro competenza) e in conformità ai principi generali di cui all'art. 5 del Regolamento. In particolare, TRANSPARENCY dovrà verificare che gli Incaricati applichino tutte le disposizioni in materia di sicurezza relativa alla custodia delle parole chiave (trattamenti elettronici) e che conservino in luogo sicuro i supporti non informatici contenenti eventuali atti o documenti con categorie particolari di dati (dati sensibili o giudiziari) o la loro riproduzione, adottando contenitori con serratura (trattamenti cartacei di dati sensibili);
f) assicurare l'adozione, l'implementazione e l'utilizzo delle misure tecniche ed organizzative di cui all'**Appendice 2**, nonché di tutte le ulteriori misure tecniche ed

organizzative che si dovessero rendere necessarie per proteggere i Dati Personali (compresi i Dati Giudiziari e le Categorie Particolari di Dati Personali, qualora presenti) ai sensi degli artt. 25 e 32 del Regolamento, in particolare contro:

- distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a Dati Personali trasmessi, conservati o comunque trattati.
- Trattamento dei Dati Personali non consentito o non conforme alle finalità delle operazioni di Trattamento.

g) applicare le misure di sicurezza di cui al punto precedente al fine di garantire:
   - se del caso, la pseudonimizzazione o la cifratura dei dati personali;
   - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

h) adottare ed aggiornare, secondo criteri di diligenza professionale, protocolli di *disaster recovery e business continuity*, garantendo, in ogni caso, che i Dati Personali siano conservati con regolari operazioni di backup cifrati;

i) implementare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento, trasmettendo tempestivamente a WBS la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito adottate; a tal fine, TRANSPARENCY informerà immediatamente WBS qualora, a suo parere, un'istruzione violi le Leggi applicabili in materia di protezione dei Dati Personali;

j) mettere a disposizione di WBS tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento; inoltre, consentirà e contribuirà alle attività di revisione, comprese eventuali ispezioni. A tale scopo TRANSPARENCY riconosce a WBS, e agli incaricati dal medesimo, il diritto di accedere ai locali di sua pertinenza ove hanno svolgimento le operazioni di Trattamento o dove sono custoditi dati o documentazione relativi al presente Accordo TDP. In ogni caso WBS si impegna a mantenere la riservatezza sulle informazioni raccolte durante le operazioni di verifica e pertanto a non comunicarle a soggetti terzi salvo sia necessario in adempimento di un obbligo previsto dalla legge o dal presente Accordo TDP;

k) cooperare nel riscontro alle richieste degli interessati ai sensi dell'articolo 28, par. 3, lett. e), fornendo tempestivamente le informazioni eventualmente in proprio possesso;

l) comunicare tempestivamente, senza indebito ritardo, ogni contatto o comunicazione ricevuta da un'Autorità di Controllo in relazione al Trattamento dei Dati Personali. In difetto, la responsabilità del mancato riscontro alle suddette richieste resterà esclusivamente in capo a TRANSPARENCY;

m) comunicare tempestivamente, senza indebito ritardo, ogni contatto, richiesta di informazioni o di accesso proveniente da qualunque soggetto, ente o Autorità salvo che sia imposto il segreto per legge entro 24 ore e comunque prima di dare acceso ai contenuti.

4. Obblighi di WBS

4.1. WBS è consapevole e accetta che, nella misura necessaria a consentire l'erogazione del Servizio, comunicherà i Dati Personali al Prestatore o ne consentirà a quest'ultimo l'accesso.
4.2. WBS si impegna a comunicare a TRANSPARENCY qualsiasi variazione si dovesse rendere necessaria nelle operazioni di Trattamento dei Dati Personali.
4.3. WBS dichiara, inoltre, che i Dati Personali trasmessi a TRANSPARENCY:

- sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
- in ogni caso, i Dati Personali e/o le categorie particolari di Dati Personali, eventualmente oggetto delle operazioni di trattamento affidate al Prestatore, sono raccolti e trasmessi rispettando le prescrizioni delle Leggi applicabili in materia di protezione dei Dati Personali pro tempore applicabili.

4.4. WBS assicura e garantisce che sussiste un'idonea base legale per consentire al Prestatore il Trattamento dei Dati Personali come parte della fornitura del Servizio.

5. Autorizzazione al trattamento da parte di Sub-Responsabili

5.1. WBS conferisce autorizzazione scritta generale a TRANSPARENCY a poter ricorrere a eventuali ulteriori responsabili del trattamento nella prestazione del Servizio.
5.2. Nel caso in cui TRANSPARENCY faccia ricorso a altri Sub-responsabili, la medesima si impegna a selezionare Sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti di cui alle Leggi applicabili in materia di protezione dei Dati Personali e garantisca la tutela dei diritti degli Interessati e a comunicare il nominativo del Sub-responsabile fornendo le informazioni di cui all'**Appendice 3**.

5.3. TRANSPARENCY si impegna altresì a stipulare specifici contratti o altri atti giuridici con i Sub-responsabili a mezzo dei quali siano descritti analiticamente i loro compiti e sia imposto a tali soggetti il rispetto dei medesimi obblighi di cui alle Leggi applicabili in materia di protezione dei Dati Personali ed al presente Accordo TDP, prevedendo in particolare garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa applicabile e i provvedimenti emessi dall'Autorità di Controllo.

5.4. Qualora il Sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei Dati Personali, TRANSPARENCY riconosce di conservare nei confronti di WBS l'intera responsabilità dell'adempimento degli obblighi dei Sub-responsabili coinvolti, nonché si impegna a manlevare e tenere indenne WBS da qualsiasi danno, pretesa, risarcimento, e/o sanzione possa derivare a WBS dalla mancata osservanza di tali obblighi e più in generale dalla violazione della applicabile normativa sulla tutela dei dati personali da parte di TRANSPARENCY e dei suoi sub-fornitori.

Tale manleva opererà nel rispetto delle seguenti condizioni:

tempestiva informazione a TRANSPARENCY

- la responsabilità di TRANSPARENCY opererà indipendentemente dalle coperture assicurative eventualmente applicate a WBS;
- WBS farà ogni sforzo per attenuare le conseguenze dannose della violazione e nella sua sfera di controllo.

5.5. TRANSPARENCY si impegna altresì ad informare WBS di eventuali modifiche o sostituzioni previste riguardanti i Sub-responsabili, dando così a WBS la possibilità di opporsi a tali modifiche.

5.6. Su richiesta di WBS, TRANSPARENCY fornisce tempestivamente adeguate informazioni in merito alle azioni e alle misure che TRANSPARENCY ed i suoi Sub-Responsabili hanno adottato per assicurare il rispetto delle previsioni del presente Accordo TDP.

6. Trasferimento dei Dati Personali

6.1. I dati devono essere trattati ed utilizzati preferibilmente in Italia ed esclusivamente nel territorio di uno Stato Membro dell'Unione Europea (UE).

7. Obblighi in tema di cooperazione e responsabilità

7.1. WBS e TRANSPARENCY, si impegnano a collaborare in buona fede per assicurare il rispetto delle previsioni del presente Accordo TDP, tra cui, ma non solo, il dovere di assicurare il corretto e tempestivo esercizio dei diritti dell'Interessato, gestire incidenti di

sicurezza e le Violazioni dei Dati Personali al fine di mitigare i possibili effetti avversi da essi derivanti.
7.2. WBS e TRANSPARENCY collaborano in buona fede per rendere disponibile reciprocamente e verso l'Autorità di Controllo le informazioni necessarie a dimostrare il rispetto delle Leggi applicabili in materia di protezione dei Dati Personali.

8. Restituzione dei dati e distruzione

8.1. TRANSPARENCY, restituirà o distruggerà prontamente i Dati Personali alla scadenza o risoluzione anticipata del Contratto in base alla scelta comunicata da WBS o in ogni caso su richiesta di WBS, da comunicare a TRANSPARENCY per iscritto, salvo che sussistano specifici obblighi di conservazione previsti dalla legge (inclusi, a titolo esemplificativo ma non esaustivo, quelli previsti dalle normative previste dalla Pubblica Amministrazione in riferimento ai servizi cloud, Leggi applicabili in materia di protezione dei Dati Personali o richieste provenienti dall'autorità giudiziaria), tra cui, ma non solo, quelli provenienti dall'Autorità di Controllo.
8.2. Al fine di adempiere all'obbligo di pronta restituzione di cui al precedente art. 8.1, TRANSPARENCY dovrà procedere senza ingiustificato ritardo e non oltre 7 giorni dalla richiesta di WBS. Resta inteso che TRANSPARENCY dovrà altresì procedere prontamente alla distruzione di ogni copia dei Dati Personali in suo possesso.
8.3. Nel caso in cui WBS richieda la pronta distruzione dei Dati Personali e fatto salvo quanto previsto dal successivo art. 8.4, TRANSPARENCY fornirà un'attestazione che assicuri tale pronta distruzione.
8.4. Ai fini del presente Accordo TDP e di quanto stabilito ai punti precedenti, il Cliente dichiara di optare per la scelta di distruggere i Dati Personali una volta terminato il rapporto contrattuale e trascorsi i periodi di conservazione indicati dalla legge applicabile o richiesti dalle Autorità competenti.
8.5. La presente disposizione non incide sui doveri di legge di TRANSPARENCY di conservare le registrazioni per i periodi di conservazione indicati dalla legge applicabile o richiesti dalle Autorità competenti.

9. Violazione dei Dati Personali

9.1. WBS è consapevole e acconsente che TRANSPARENCY non sarà ritenuto responsabile in caso di Violazione dei Dati Personali che non sia imputabile a colpa di quest'ultimo;
9.2. Nel caso in cui TRANSPARENCY venga a conoscenza di una Violazione dei Dati Personali, dovrà:

(a) adottare le misure tecniche e organizzative appropriate per contenere e mitigare tale Violazione dei Dati Personali;

(b) informare prontamente e senza ingiustificato ritardo WBS e, in ogni caso, non oltre ventiquattro (24) ore dalla conoscenza della Violazione dei Dati Personali, al fine di consentire a WBS l'adempimento degli obblighi di notifica e comunicazione previsti dagli artt. 33 e 34 del Regolamento e la rapida adozione delle possibili contromisure necessarie;

(c) collaborare con WBS per indagare: la natura, le categorie ed il numero approssimativo di Interessati coinvolti, le categorie ed il numero approssimativo di Dati Personali coinvolti e le probabili conseguenze di tale violazione con modalità commisurate alla serietà ed al suo impatto complessivo su WBS e sull'erogazione del Servizio previsto dal Contratto;

(d) ove le Leggi applicabili in materia di protezione dei Dati Personali richiedano la notificazione alle competenti Autorità di Controllo o la comunicazione agli Interessati della Violazione dei Dati Personali, e nel caso essa si riferisca a Dati Personali, TRANSPARENCY dovrà deferire e assumere istruzioni da WBS, che – salvo quanto previsto dalla lettera a) del presente articolo - sarà l'unico ad avere il diritto di determinare le ulteriori misure che dovranno essere adottate nel rispetto delle Leggi applicabili in materia di protezione dei Dati Personali o il diritto porre rimedio a qualsivoglia rischio, tra cui ma non solo:

   i. determinare se l'avviso debba essere fornito a qualsivoglia individuo, autorità di regolamentazione, autorità giudiziaria, enti a tutela dei consumatori o altri come richiesto dalle Leggi applicabili in materia di protezione dei Dati Personali, o richiesto a discrezione di WBS;
   ii. determinare il contenuto di tale avviso e comunicarlo ai soggetti individuati da WBS;
   iii. se sia possibile offrire all'Interessato dalla violazione qualsivoglia tipologia di rimedio riparatorio, nonché la natura e l'estensione di tale rimedio.

10. Trasmissione

10.1. I Dati Personali trasmessi da TRANSPARENCY in relazione al Servizio attraverso Internet dovranno essere cifrati in modo appropriato in osservanza delle disposizioni di cui all'**Appendice 2**. Le Parti sono altresì consapevoli che la sicurezza delle trasmissioni su Internet non potrà essere completamente garantita.

11. Durata e validità

11.1. Il presente Accordo TDP avrà la medesima durata del Contratto di cui il presente documento costituisce un allegato. Qualora questo venisse meno o perdesse efficacia e per qualsiasi motivo, anche il presente Accordo TDP verrà automaticamente meno, senza bisogno di comunicazioni o revoche, e TRANSPARENCY non sarà più legittimata a Trattare i Dati Personali cessando lo status di Sub-Responsabile.
11.2. Con il presente Accordo TDP, WBS e TRANSPARENCY intendono espressamente revocare e sostituire ogni altra eventuale nomina e accordo relativo ai medesimi prodotti per qualsivoglia tipologia di Dati Personali.

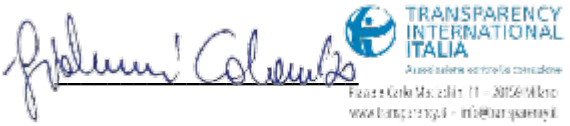
Milano, 14 dicembre 2021

Per conto di WBS:

Giovanni Pellerano

Giovanni Pellerano
Legale Rappresentante

Per conto di TRANSPARENCY:



Giovanni Colombo, Direttore
Legale Rappresentante

APPENDICE 1

Categorie di interessati: i Dati Personali riguardano le seguenti categorie di Interessati: personale e collaboratori di WBS; referenti di Clienti Titolari del trattamento che attivano il Servizio di Whistleblowing Digitale realizzato da WBS, soggetti riceventi le segnalazioni (Responsabili Anticorruzione, Organismi di Vigilanza, Audit, ecc.); soggetti che inviano le segnalazioni (dipendenti, collaboratori, consulenti, clienti, fornitori); Terzi indeterminati.

Tipo di Dati Personali oggetto di trattamento: i Dati Personali oggetto di trattamento si riferiscono alle seguenti tipologie di dati:

- Dati comuni: dati anagrafici, di contatto, professionali, indirizzi IP, log, ID utenti, codici di identificazione, dati bancari;
- Categorie particolari di Dati Personali: dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti allegati, relativi alla salute eventualmente contenuti nella segnalazione.

Natura e finalità del trattamento: il trattamento dei Dati Personali è obbligatorio per l'esecuzione del Servizio oggetto del Contratto.

Descrizione delle attività di trattamento: operazioni di trattamento necessarie per l'esecuzione del Servizio oggetto del Contratto.

Modalità di Trattamento

I Dati Personali sono trattati secondo modalità cartacea e elettronica.

APPENDICE 2

1. Descrizione delle misure di sicurezza tecniche ed organizzative

TRANSPARENCY si impegna a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte.

2. Informazioni sulle misure di sicurezza

2.1 Gestione della sicurezza delle informazioni

TRANSPARENCY si impegna a definire una serie di politiche e misure per chiarire gli obiettivi al fine di supportare la sicurezza delle informazioni.

2.2 Organizzazione della sicurezza delle informazioni

2.2.1 Organizzazione interna

TRANSPARENCY si impegna a garantire che l'organizzazione definisca i ruoli e le responsabilità per la sicurezza delle informazioni e assegnarli singolarmente a soggetti determinati. Ove necessario, i compiti devono essere separati per ruoli e persone al fine di evitare conflitti di interesse e prevenire attività inappropriate.

2.2.2 Dispositivi mobili e telelavoro

TRANSPARENCY si impegna a definire una Policy di sicurezza e adeguati controlli per i dispositivi mobili (come laptop, tablet, PC, dispositivi indossabili, smartphone, strumenti USB e altri) e per il telelavoro (come coloro che lavorano da casa, quelli che viaggiano assiduamente e le postazioni di lavoro da remoto/virtuali).

2.2.3 Sicurezza delle risorse umane

Prima dell'instaurazione del rapporto di lavoro

TRANSPARENCY si impegna a prendere in considerazione le responsabilità della sicurezza delle informazioni durante l'assunzione di dipendenti, collaboratori e personale temporaneo (ad esempio attraverso adeguate descrizioni sulle mansioni da svolgere, controlli pre-assunzione) e ad inserirle all'interno dei contratti (ad esempio con termini e condizioni del rapporto di lavoro e sottoscrizione di ulteriori accordi volti a definire ruoli e responsabilità in tema di sicurezza, obblighi di conformità, ecc.).

Durante il rapporto di lavoro

TRANSPARENCY si impegna a garantire che i dipendenti e i collaboratori siano consapevoli e motivati a rispettare i loro obblighi per garantire la sicurezza delle informazioni.

Conclusione o modifiche al rapporto di lavoro

TRANSPARENCY si impegna a gestire gli aspetti relativi alla sicurezza al momento dell'uscita di una persona dall'organizzazione, o nelle ipotesi di modifiche significative al ruolo ricoperto, come la restituzione delle informazioni e delle apparecchiature aziendali in possesso del soggetto uscente, l'aggiornamento dei permessi di accesso, nonché il rispetto dei perduranti obblighi relativi alle informazioni riservate ed ai diritti di proprietà intellettuale, ai termini contrattuali, ecc. ed anche ai doveri etici.

2.2.4 Gestione delle risorse del patrimonio aziendale

Responsabilità delle risorse del patrimonio aziendale

TRANSPARENCY si impegna a inventariare tutte le informazioni relative alle risorse del patrimonio aziendale e ad identificare i relativi soggetti di riferimento al fine di individuare le responsabilità per la loro sicurezza. TRANSPARENCY si impegna altresì a definire una Policy per un "uso corretto" delle stesse e a far rientrare le risorse all'interno dell'organizzazione al momento dell'uscita dei soggetti coinvolti.

Classificazione delle informazioni

TRANSPARENCY si impegna a classificare e a catalogare le informazioni dai rispettivi soggetti di riferimento in linea con quanto previsto dalle esigenze di sicurezza, nonché a trattarle in modo appropriato.

Gestione dei media

TRANSPARENCY si impegna a gestire, controllare, modificare ed utilizzare le informazioni conservate sui media in modo tale da non comprometterne il loro contenuto.

2.2.5 Controllo degli accessi

Requisiti aziendali per il controllo degli accessi

TRANSPARENCY si impegna a documentare chiaramente i requisiti previsti dall'organizzazione per controllare l'accesso alle informazioni relative al patrimonio aziendale in una Policy per il controllo degli accessi e delle relative procedure. TRANSPARENCY si impegna a garantire che l'accesso alla rete e le connessioni prevedano delle limitazioni.

Gestione dell'accesso degli utenti

TRANSPARENCY si impegna a garantire che l'allocazione dei diritti d'accesso da parte degli utenti sia controllata dalla registrazione iniziale dell'utente fino alla rimozione del profilo quando esso non sia più necessario, incluse speciali restrizioni per i diritti di accesso privilegiato e la gestione delle password (definita come "informazione di autenticazione segreta"); TRANSPARENCY si impegna, peraltro, a procedere regolarmente alla revisione e all'aggiornamento dei diritti di accesso.

Responsabilità degli utenti

TRANSPARENCY si impegna a garantire che gli utenti siano consapevoli delle loro responsabilità attraverso il mantenimento di un effettivo controllo degli accessi, ad es. scegliendo password complesse e mantenendole riservate.

Sistemi e applicazioni per il controllo degli accessi

TRANSPARENCY si impegna a garantire che l'accesso alle informazioni sia limitato coerentemente a quanto previsto dalla Policy sul controllo degli accessi, ad es. attraverso autenticazioni sicure, gestione delle password, controllo delle utilità privilegiate e limitazioni all'accesso ai codici sorgente dei programmi.

2.2.6 Crittografia

Controllo crittografico

TRANSPARENCY si impegna a definire una Policy sull'uso della cifratura dei dati, oltre ad autenticazioni criptate e controlli di integrità, come firme digitali e messaggi con codici di autenticazione, nonché una gestione delle chiavi di cifratura.

2.2.7 Sicurezza fisica e ambientale

Aree sicure

TRANSPARENCY si impegna a garantire che un perimetro fisico e una recinzione, con controllo fisico degli accessi e procedure operative, sia in grado di proteggere i locali, gli uffici, le stanze, le aree di carico/scarico da accessi non autorizzati. TRANSPARENCY si impegna altresì a garantire la consulenza di uno specialista per quanto riguarda le misure di protezione contro incendi, allagamenti, terremoti, esplosioni, ecc.

Apparecchiature

TRANSPARENCY si impegna a rendere sicuri e manutenuti le apparecchiature (intese perlopiù come apparecchiatura in ambito ICT), i servizi di supporto e il cablaggio. TRANSPARENCY si impegna a garantire che:
a) l'apparecchiatura e le informazioni non escano dal loro luogo di riferimento se non previa autorizzazione, e in ogni caso siano adeguatamente protette sia all'interno che all'esterno del loro luogo di riferimento;
b) le informazioni siano distrutte prima di procedere allo smaltimento o al riciclo dei dispositivi su cui erano conservate;
c) le apparecchiature non protette siano rese sicure e sia previsto un apposito spazio ed una chiara Policy di verifica.

2.2.8 Operazioni di sicurezza

Procedure e responsabilità operative
TRANSPARENCY si impegna: a documentare le procedure e le responsabilità operanti per l'area IT; a controllare i cambiamenti alle infrastrutture ed ai sistemi IT; a gestire i singoli poteri e le relative prestazioni; a separare i sistemi di sviluppo, quelli di verifica e quelli operativi.

Protezione da malware
TRANSPARENCY si impegna a garantire il controllo dei malware, comprensivo di un'idonea consapevolezza sul punto da parte degli utenti.

Backup
TRANSPARENCY si impegna a eseguire idonei backup e a custodirli coerentemente ad una policy per i backup.

Autenticazione e monitoraggio
TRANSPARENCY si impegna a garantire che le attività, le eccezioni, gli errori e gli eventi relativi alla sicurezza delle informazioni da parte degli utenti del sistema e degli amministratori/operatori avvengano previo inserimento delle credenziali di autenticazione adeguatamente protette. TRANSPARENCY si impegna altresì a garantire che gli orologi siano sincronizzati.

Controllo di software operativi
TRANSPARENCY si impegna a garantire che l'installazione di software sui sistemi operativi sia controllata.

Gestione delle vulnerabilità tecniche

TRANSPARENCY si impegna a garantire che le vulnerabilità tecniche siano corrette con idonee patch e che siano previste regole per l'installazione dei software da parte degli utenti.

Considerazioni sull'audit per le informazioni di sistema

TRANSPARENCY si impegna a garantire che l'audit per l'area IT sia programmato e controllato per minimizzare l'effetto avverso sui sistemi di produzione o l'accesso abusivo ai dati.

2.2.9 Sicurezza delle comunicazioni

Gestione della sicurezza della rete

TRANSPARENCY si impegna a garantire che le reti e i servizi in rete siano resi sicuri, ad esempio attraverso la loro separazione.

Trasferimento delle informazioni

TRANSPARENCY si impegna a definire policy, procedure ed accordi (ad es. accordi di riservatezza) relativi al trasferimento delle informazioni verso/da terze parti, compresi i messaggi elettronici.

2.2.10 Acquisizione, sviluppo e manutenzione del sistema

Requisiti di sicurezza dei sistemi di informazione

TRANSPARENCY si impegna a garantire che i requisiti per il controllo di sicurezza siano analizzati e specificati, comprese le applicazioni web e le transazioni.

Sicurezza nello sviluppo e processi di supporto

TRANSPARENCY si impegna: a definire in una Policy le regole che governano la sicurezza dello sviluppo dei software/sistemi; a garantire che siano controllate le modifiche al sistema (sia per le applicazioni che per i sistemi operativi); a garantire che i pacchetti software non siano teoricamente modificati e che siano osservati i principi di sicurezza ingegneristica; a rendere sicuro l'ambiente di sviluppo e controllare lo sviluppo esternalizzato; a garantire che la sicurezza del sistema sia testata e che siano definiti criteri di ammissibilità che includano gli aspetti di sicurezza.

Test di verifica dei dati

TRANSPARENCY si impegna a garantire che i test di verifica dei dati siano accuratamente selezionati/generati e controllati.

2.2.11 Rapporti con i fornitori

Sicurezza delle informazioni nei rapporti coi fornitori

TRANSPARENCY si impegna a definire policy, procedure, sistemi di consapevolezza volti a proteggere le informazioni dell'organizzazione che siano accessibili ai soggetti esterni operanti nell'area IT e ad altri fornitori esterni per l'intera catena di fornitura, concordata nei contratti o negli accordi.

Gestione dei servizi resi dal fornitore

TRANSPARENCY si impegna a garantire che l'erogazione dei servizi resi dal fornitore sia monitorata e rivista/verificata in relazione al contratto/accordo e che le modifiche al servizio siano controllate.

2.2.12 Gestione degli incidenti alle informazioni di sicurezza

Gestione degli incidenti alle informazioni di sicurezza e miglioramenti

Dovrebbero essere previste responsabilità e procedure (report, valutazioni, rispondere a e imparare da) volte a gestire in modo coerente ed efficace gli eventi, gli incidenti e le debolezze relative alle informazioni di sicurezza, anche al fine di conservare prove valide in eventuali giudizi.

2.2.13 Aspetti della sicurezza delle informazioni relativi alla continuità aziendale

Continuità della sicurezza delle informazioni

TRANSPARENCY si impegna a garantire che la continuità della sicurezza delle informazioni sia pianificata, implementata e revisionata come parte integrante del sistema organizzativo di continuità aziendale.

Ridondanze

TRANSPARENCY si impegna a garantire che le strutture IT siano sufficientemente ridondanti per soddisfare i requisiti di disponibilità.

2.2.14 Conformità

Conformità ai requisiti legali e contrattuali

TRANSPARENCY si impegna a garantire che l'organizzazione identifichi e documenti i suoi obblighi alle autorità esterne e ad altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile, le informazioni relative alla privacy/comunque idonee a consentire l'identificazione personale e la crittografia.

Revisione della sicurezza delle informazioni

TRANSPARENCY si impegna a garantire che i progetti dell'organizzazione relativamente alla sicurezza delle informazioni siano revisionati (verificati tramite audit) con modalità tali da garantire l'indipendenza della valutazione e rendicontate alla Direzione. TRANSPARENCY si impegna altresì a garantire che i manager revisionino periodicamente la conformità dei dipendenti e dei sistemi alle policy di sicurezza, alle procedure, ecc., e promuovano azioni correttive ove necessario.

APPENDICE 3

(Elenco dei Sub-Responsabili)

La tabella dei Sub-Responsabili deve essere compilata di volta in volta da TRANSPARENCY e trasmessa a WBS in modo che possa opporsi all'impiego di nuovi Sub-Responsabili ai sensi dell'art. 28 del Regolamento.

Sub-Responsabili (indicare: luogo di stabilimento e dettagli di contatto) *Ad es., Nome della società, Indirizzo, soggetto responsabile in materia di protezione dei Dati Personali e dettagli di contatto*	**Paese/i in cui i Dati Personali sono trattati e finalità** *Ad es., Italia per hosting e Francia per backup*
non previsti	

ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI

AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679

("REGOLAMENTO")

TRA

Whistleblowing Solutions Impresa Sociale S.r.l.

(Titolare del Trattamento)

E

Seeweb S.r.l.

(Responsabile del Trattamento)

In relazione alla fornitura specifica dei seguenti prodotti:

Foundation Server PRO (fs20585, fs20687),

Cloud Data Protection (cdp000132),

Appliance VPN OPNsense (vm9619)

1. Premessa

1.1. Premesso che:

A. Le vigenti disposizioni in materia di Trattamento dei Dati Personali prevedono che qualora un Trattamento sia effettuato per conto di **Whistleblowing Solutions Impresa Sociale S.r.l.** ("**WBS**"), da una persona fisica o giuridica, una pubblica amministrazione o qualsiasi altro ente o associazione quale Responsabile del Trattamento, WBS in qualità di Titolare ricorra a soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento dei Dati Personali, ivi compreso il profilo della sicurezza; pertanto il Responsabile del Trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti richiesti dalle Leggi applicabili in materia di protezione dei Dati Personali pro tempore vigenti in materia e garantisca la tutela dei diritti dell'Interessato.
Il persente Accordo comprende anche il Trattamento di Dati Personali che Whistleblowing Solutions Impresa Sociale S.r.l. effettua quale Responsabile del trattamento per conto di propri Clienti, Titolari del trattamento.

B. SEEWEB S.r.l. ("**SEEWEB**") dichiara di avere tutte le competenze tecniche e organizzative idonee, ai sensi e per gli effetti dell'art. 28 del Regolamento, al ruolo di Responsabile del Trattamento dei Dati Personali per conto del Titolare per l'esecuzione del Contratto di cui il presente documento costituisce un allegato.

C. WBS e SEEWEB si danno reciprocamente atto che:

a) il Cliente (WBS) è Titolare dei Dati Personali determinando le finalità e le modalità del loro Trattamento nell'erogazione del Servizio oggetto del Contratto. In taluni casi il Cliente (WBS) è Responsabile del Trattamento dei Dati dei propri Clienti, Titolari del Trattamento;
b) il Prestatore (SEEWEB) è Responsabile dei Dati Personali Trattati in esecuzione del Servizio oggetto del Contratto; in particolare, pertanto, i compiti e le responsabilità di SEEWEB sono strettamente legati al diretto adempimento delle obbligazioni assunte nell'ambito del Contratto, con esclusione di ogni altra responsabilità. Nei casi in cui il Cliente (WBS) è Responsabile del Trattamento, il Prestatore (SEEWEB) agirà quale ulteriore Responsabile dei Dati Personali Trattati (Sub-Responsabile);
c) il presente accordo e le sue appendici (congiuntamente denominati "Accordo per il Trattamento dei Dati Personali" o anche "Accordo TDP"), sono sottoscritti da WBS e SEEWEB al fine di dettagliare le istruzioni e regolare il rapporto tra il Titolare e il Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento, anche con riferimento ai rispettivi diritti e obblighi relativi al Trattamento dei Dati Personali posto in essere dal Responsabile del Trattamento ed in particolare per stabilire misure di

sicurezza e procedure idonee per procedere al legittimo Trattamento dei Dati Personali; il presente Accordo TDP è a titolo gratuito in quanto collegato alla fornitura del Servizio;

d) con il presente Accordo TDP, il Titolare affida al Responsabile del Trattamento tutte ed esclusivamente le operazioni di Trattamento dei Dati Personali necessarie per dare piena esecuzione al Servizio, come descritto nel Contratto e nei suoi allegati. In caso di danni derivanti dal Trattamento dei Dati Personali posto in essere dal Responsabile del Trattamento, questi ne risponderà solo qualora non abbia adempiuto agli obblighi derivanti dalle Leggi applicabili in materia di protezione dei Dati Personali specificatamente diretti ai responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare.

D. In particolare, la finalità perseguita, la tipologia, e le modalità del Trattamento dei Dati Personali sono descritti nell'**Appendice 1.**

E. In caso di contrasto o incongruenze per quanto riguarda gli accordi tra le Parti in materia di protezione dei Dati Personali tra il presente Accordo TDP e il Contratto, prevale quanto stabilito nell'Accordo TDP ed in eventuali accordi integrativi o modificativi di quest'ultimo.

F. La presente premessa forma parte integrante dell'Accordo TDP.

2. Definizioni

2.1. Salvo che sia diversamente definito nel presente Accordo TDP, tutti i termini utilizzati nel presente documento e nelle sue appendici hanno il significato loro attribuito nel Contratto.

"**Accordo per il Trattamento dei Dati Personali" o "Accordo TDP**" indica il presente accordo per il Trattamento dei Dati Personali comprensivo delle Appendici 1, 2 e 3, nonché di eventuali accordi modificativi o integrativi;

"**Autorità di Controllo**" indica ogni autorità competente a vigilare ed assicurare l'applicazione delle Leggi applicabili in materia di protezione dei Dati Personali con riferimento al Trattamento dei Dati Personali svolti per mezzo del Servizio;

"Categorie Particolari di Dati Personali" indica i Dati Personali che rivelino: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il Trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

"**Contratto**" indica il Contratto per i prodotti "**Foundation Server PRO (fs20585, fs20687), Cloud Data Protection (cdp000132), Appliance VPN OPNsense (vm9619)"** qualificati da AgID per erogare servizi IaaS alla Pubblica Amministrazione;

“Dati Giudiziari” indica i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;

“**Dati Personali del Cliente**” indica i Dati Personali trattati in relazione al Servizio fornito dal Responsabile per conto del Cliente per l’esecuzione del Contratto;

“Dati Personali” significa qualsiasi informazione riguardante una persona fisica identificata o identificabile (“Interessato”) oggetto di Trattamento da parte del Prestatore per conto del Titolare in esecuzione del Contratto; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; al fine di evitare contrasti interpretativi, ha in ogni caso il significato previsto dal Regolamento e dalle Leggi applicabili in materia di protezione dei Dati Personali;

“Diritti dell’Interessato” sono i diritti riconosciuti all’Interessato dalle Leggi applicabili in materia di protezione dei Dati Personali come, nei limiti di applicabilità del Regolamento, ad esempio, il diritto di chiedere al Titolare l’accesso, la rettifica o la cancellazione dei Dati Personali, il diritto alla limitazione del Trattamento dei dati dell’Interessato o il diritto di opposizione al Trattamento, nonché il diritto alla portabilità dei dati;

“**Elenco dei Sub-Responsabili**” indica l’elenco disponibile nell’**Appendice 3**;

“Incaricato/i” il personale, dipendenti, collaboratori a qualsiasi titolo del Prestatore che abbiano accesso ai Dati Personali e agiscono sotto l’autorità del Responsabile del Trattamento ai sensi dell’art. 29 del Regolamento;

“Interessato/i” ha il significato previsto dal Regolamento;

“Leggi applicabili in materia di protezione dei Dati Personali” indica, negli Stati membri dell’Unione Europea, il Regolamento e le complementari legislazioni nazionali in materia di protezione dei Dati Personali, comprensivi di ogni orientamento e/o *code of pratice* emessi dalla competente Autorità di Controllo all’interno dell’Unione Europea (inclusi i provvedimenti e/o delle Autorizzazioni e/o Linee Guida del Garante per la protezione dei dati personali in quanto applicabili); e/o, negli Stati extra UE, ogni vigente legislazione in materia di protezione dei Dati Personali relativa alla tutela ed al legittimo Trattamento di Dati Personali;

“Regolamento” indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE;

“Responsabile del Trattamento” indica la persona fisica o giuridica, la pubblica autorità, l’organismo o altro ente che effettua un Trattamento dei Dati Personali per conto del Titolare. Ai fini del presente Accordo TDP, il Responsabile è **SEEWEB** (anche “**Prestatore**”); si precisa

che la responsabilità gravante sul Prestatore include il trattamento dei Dati Personali di cui il Cliente (WBS) sia a sua volta Responsabile, rispetto ai quali il Prestatore quindi assume la qualità di Sub-Responsabile;

"**Servizio**" indica il servizio oggetto del Contratto di cui il presente Accordo TDP costituisce allegato;

"**Sub-Responsabile**" indica un organismo individuato dal Responsabile per assisterlo nel (o che intraprenda direttamente qualsivoglia) Trattamento dei Dati Personali nel rispetto delle obbligazioni previste dal Responsabile e di cui al presente Accordo TDP, che sia stato autorizzato dal Titolare ai sensi dell'Art. 5 del presente Accordo TDP;

"Titolare" indica la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che, da solo o congiuntamente con altri soggetti, determini le finalità e le modalità del Trattamento dei Dati Personali. Ai fini del presente Accordo TDP, il Titolare è **WBS** (anche "**Cliente**);

"Trattare" o "**Trattamento**" significa qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come 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;

"**UE**" indica l'Unione Europea;

"Violazione dei Dati Personali" indica la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

3. Obblighi del Responsabile del trattamento

3.1. Il Responsabile del Trattamento, per quanto di competenza, è tenuto, in forza di legge e di contratto, per sé e per gli Incaricati e per qualunque soggetto collabori con la sua attività, al rispetto delle Leggi applicabili in materia di protezione dei Dati Personali.

3.2. Fatti salvi gli obblighi stabiliti da altre disposizioni del presente Accordo TDP, il Responsabile del Trattamento è obbligato a:

a) trattare i Dati Personali solo per quanto strettamente necessario all'erogazione del Servizio e solo limitatamente alla conduzione tecnico funzionale dei sistemi/servizi oggetto del Contratto;
b) rispettare le istruzioni impartite dal Titolare per iscritto con il presente Accordo TDP e con eventuali accordi scritti successivi, avvertendo il Titolare qualora ritenga che le

istruzioni impartite si pongano in violazione delle Leggi applicabili in materia di protezione dei Dati Personali;

c) contestualmente alla designazione, fornire adeguate istruzioni scritte agli Incaricati circa le modalità del Trattamento dei Dati Personali in ottemperanza a quanto disposto dalle Leggi applicabili in materia di protezione dei Dati Personale e dal presente Accordo TDP. A titolo esemplificativo e non esaustivo, il Responsabile del Trattamento, nel designare per iscritto gli Incaricati, dovrà prescrivere che essi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Inoltre, ove occorrer possa, per i Trattamenti effettuati per fornire il Servizio dagli Incaricati con mansioni di "Amministratore di Sistema", il Responsabile del Trattamento è tenuto altresì al rispetto del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (modificato in base al provvedimento del 25 giugno 2009) e delle Leggi applicabili in materia di protezione dei Dati Personali pro tempore applicabili relative alla disciplina sugli amministratori di sistema. La versione aggiornata dell'elenco contenente gli estremi identificativi (nome, cognome, funzione o area organizzativa di appartenenza) degli Amministratori di Sistema dovrà essere consegnato senza indugio a semplice richiesta anche solo verbale di WBS, a quest'ultimo e/o alle competenti Autorità e ad eventuali ulteriori terzi aventi diritto;

d) vincolare gli Incaricati alla riservatezza, anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto, in relazione alle operazioni di Trattamento da essi eseguite;

e) verificare che gli Incaricati di cui al punto precedente applichino tutte le disposizioni in materia di sicurezza adottate ai sensi dell'art. 32 del Regolamento (per quanto di loro competenza) e in conformità ai principi generali di cui all'art. 5 del Regolamento. In particolare, il Responsabile del Trattamento dovrà verificare che gli Incaricati applichino tutte le disposizioni in materia di sicurezza relativa alla custodia delle parole chiave (trattamenti elettronici) e che conservino in luogo sicuro i supporti non informatici contenenti eventuali atti o documenti con categorie particolari di dati (dati sensibili o giudiziari) o la loro riproduzione, adottando contenitori con serratura (trattamenti cartacei di dati sensibili);

f) assicurare l'adozione, l'implementazione e l'utilizzo delle misure tecniche ed organizzative di cui all'**Appendice 2**, nonché di tutte le ulteriori misure tecniche ed organizzative che si dovessero rendere necessarie per proteggere i Dati Personali (compresi i Dati Giudiziari e le Categorie Particolari di Dati Personali, qualora presenti) ai sensi degli artt. 25 e 32 del Regolamento, in particolare contro:

- distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a Dati Personali trasmessi, conservati o comunque trattati.
- Trattamento dei Dati Personali non consentito o non conforme alle finalità delle operazioni di Trattamento;

Al fine in particolare di prevenire il Trattamento non consentito di Dati Personali, il Responsabile si impegna a comunicare tempestivamente al Titolare la necessità di revocare il profilo autorizzativo del proprio personale che non ha più accesso ai sistemi del Titolare.

g) applicare le misure di sicurezza di cui al punto precedente al fine di garantire:
   - se del caso, la pseudonimizzazione o la cifratura dei dati personali;
   - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
h) adottare ed aggiornare, secondo criteri di diligenza professionale, protocolli di *disaster recovery e business continuity*, garantendo, in ogni caso, che i Dati Personali siano conservati con regolari operazioni di backup cifrati;
i) implementare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento, trasmettendo tempestivamente al Titolare la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito adottate; a tal fine, il Responsabile del Trattamento informerà immediatamente il Titolare qualora, a suo parere, un'istruzione violi le Leggi applicabili in materia di protezione dei Dati Personali;
j) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento; inoltre, consentirà e contribuirà alle attività di revisione, comprese eventuali ispezioni, realizzati dal Titolare o da un altro soggetto da questi incaricato. A tale scopo il Responsabile del Trattamento riconosce al Titolare, e agli incaricati dal medesimo, il diritto di accedere ai locali di sua pertinenza ove hanno svolgimento le operazioni di Trattamento o dove sono custoditi dati o documentazione relativi al presente Accordo TDP. In ogni caso il Titolare si impegna a mantenere la riservatezza sulle informazioni raccolte durante le operazioni di verifica e pertanto a non comunicarle a soggetti terzi salvo sia necessario in adempimento di un obbligo previsto dalla legge o dal presente Accordo TDP;

k) cooperare con il Titolare del Trattamento nel riscontro alle richieste degli interessati ai sensi dell'articolo 28, par. 3, lett. e), fornendo tempestivamente le informazioni eventualmente in proprio possesso;
l) comunicare tempestivamente, senza indebito ritardo, ogni contatto o comunicazione ricevuta da un'Autorità di Controllo in relazione al Trattamento dei Dati Personali. In difetto, la responsabilità del mancato riscontro alle suddette richieste resterà esclusivamente in capo al Responsabile del Trattamento;
m) comunicare tempestivamente, senza indebito ritardo, ogni contatto, richiesta di informazioni o di accesso proveniente da qualunque soggetto, ente o Autorità salvo che sia imposto il segreto per legge entro 24 ore e comunque prima di dare acceso ai contenuti.

4. Obblighi del Titolare

4.1. Il Cliente è consapevole e accetta che, nella misura necessaria a consentire l'erogazione del Servizio, comunicherà i Dati Personali di cui è Titolare al Prestatore o ne consentirà a quest'ultimo l'accesso.
4.2. Il Titolare si impegna a comunicare al Responsabile del Trattamento qualsiasi variazione si dovesse rendere necessaria nelle operazioni di Trattamento dei Dati Personali.
4.3. Il Cliente dichiara, inoltre, che i Dati Personali trasmessi al Responsabile:

- sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
- in ogni caso, i Dati Personali e/o le categorie particolari di Dati Personali, oggetto delle operazioni di trattamento affidate al Prestatore, sono raccolti e trasmessi rispettando le prescrizioni delle Leggi applicabili in materia di protezione dei Dati Personali pro tempore applicabili.

4.4. Il Cliente assicura e garantisce che sussiste un'idonea base legale per consentire al Prestatore il Trattamento dei Dati Personali come parte della fornitura del Servizio.

5. Autorizzazione al trattamento da parte di Sub-Responsabili

5.1. Il Titolare conferisce autorizzazione scritta generale al Responsabile del Trattamento a poter ricorrere a eventuali ulteriori responsabili del trattamento nella prestazione del Servizio.
5.2. Nel caso in cui il Responsabile del Trattamento faccia ricorso a Sub-responsabili, il medesimo si impegna a selezionare Sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti di cui alle Leggi

applicabili in materia di protezione dei Dati Personali e garantisca la tutela dei diritti degli Interessati e a comunicare il nominativo del Sub-responsabile fornendo le informazioni di cui all'**Appendice 3**.

5.3. Il Responsabile del Trattamento si impegna altresì a stipulare specifici contratti o altri atti giuridici con i Sub-responsabili a mezzo dei quali siano descritti analiticamente i loro compiti e sia imposto a tali soggetti il rispetto dei medesimi obblighi di cui alle Leggi applicabili in materia di protezione dei Dati Personali ed al presente Accordo TDP, prevedendo in particolare garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa applicabile e i provvedimenti emessi dall'Autorità di Controllo.

5.4. Qualora il Sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei Dati Personali, il Responsabile del Trattamento riconosce di conservare nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dei Sub-responsabili coinvolti, nonché si impegna a manlevare e tenere indenne il Titolare da qualsiasi danno, pretesa, risarcimento, e/o sanzione possa derivare al Titolare dalla mancata osservanza di tali obblighi e più in generale dalla violazione della applicabile normativa sulla tutela dei dati personali da parte del Responsabile e dei suoi sub-fornitori.

Tale manleva opererà nel rispetto nelle seguenti condizioni:

- tempestiva informazione al Responsabile
- la responsabilità del Responsabile opererà indipendentemente dalle coperture assicurative eventualmente applicate al Titolare;
- il Titolare farà ogni sforzo per attenuare le conseguenze dannose della violazione e nella sua sfera di controllo.

5.5. Il Responsabile del Trattamento si impegna altresì ad informare il Titolare di eventuali modifiche o sostituzioni previste riguardanti i Sub-responsabili, dando così al Titolare la possibilità di opporsi a tali modifiche.

5.6. Su richiesta del Titolare, il Responsabile fornisce tempestivamente al Titolare adeguate informazioni in merito alle azioni e alle misure che il Responsabile ed i suoi Sub-Responsabili hanno adottato per assicurare il rispetto delle previsioni del presente Accordo TDP.

6. Trasferimento dei Dati Personali

6.1. I dati devono essere trattati ed utilizzati preferibilmente in Italia ed esclusivamente nel territorio di uno Stato Membro dell'Unione Europea (UE).

7. Obblighi in tema di cooperazione e responsabilità

7.1. Il Cliente e il Prestatore, si impegnano a collaborare in buona fede per assicurare il rispetto delle previsioni del presente Accordo TDP, tra cui, ma non solo, il dovere di assicurare il corretto e tempestivo esercizio dei diritti dell'Interessato, gestire incidenti di sicurezza e le Violazioni dei Dati Personali al fine di mitigare i possibili effetti avversi da essi derivanti.
7.2. Il Cliente e il Prestatore collaborano in buona fede per rendere disponibile reciprocamente e verso l'Autorità di Controllo le informazioni necessarie a dimostrare il rispetto delle Leggi applicabili in materia di protezione dei Dati Personali.

8. Restituzione dei dati e distruzione

8.1. Il Responsabile del Trattamento, senza porre costi aggiuntivi a carico del Titolare, restituirà o distruggerà prontamente i Dati Personali alla scadenza o risoluzione anticipata del Contratto in base alla scelta comunicata dal Titolare o in ogni caso su richiesta del Titolare, da comunicare al Responsabile del Trattamento per iscritto, salvo che sussistano specifici obblighi di conservazione previsti dalla legge (inclusi, a titolo esemplificativo ma non esaustivo, quelli previsti dalle normative previste dalla Pubblica Amministrazione in riferimento ai servizi cloud, Leggi applicabili in materia di protezione dei Dati Personali o richieste provenienti dall'autorità giudiziaria), tra cui, ma non solo, quelli provenienti dall'Autorità di Controllo.
8.2. Al fine di adempiere all'obbligo di pronta restituzione di cui al precedente art. 8.1, il Responsabile del Trattamento dovrà procedere senza ingiustificato ritardo e non oltre 7 giorni dalla richiesta del Titolare. Resta inteso che il Responsabile del Trattamento dovrà altresì procedere prontamente alla distruzione di ogni copia dei Dati Personali in suo possesso.
8.3. Nel caso in cui il Titolare richieda la pronta distruzione dei Dati Personali e fatto salvo quanto previsto dal successivo art. 8.4, il Responsabile fornirà un'attestazione che assicuri tale pronta distruzione.
8.4. Ai fini del presente Accordo TDP e di quanto stabilito ai punti precedenti, il Cliente dichiara di optare per la scelta di distruggere i Dati Personali una volta terminato il rapporto contrattuale e trascorsi i periodi di conservazione indicati dalla legge applicabile o richiesti dalle autorità competenti.
8.5. La presente disposizione non incide sui doveri di legge del Responsabile del Trattamento di conservare le registrazioni per i periodi di conservazione indicati dalla legge applicabile o richiesti dalle autorità competenti.

9. Violazione dei Dati Personali

9.1. Il Titolare è consapevole e acconsente che il Responsabile del Trattamento non sarà ritenuto responsabile in caso di Violazione dei Dati Personali che non sia imputabile a colpa di quest'ultimo;

9.2. Nel caso in cui il Responsabile venga a conoscenza di una Violazione dei Dati Personali, dovrà:

(a) adottare le misure tecniche e organizzative appropriate per contenere e mitigare tale Violazione dei Dati Personali;

(b) informare prontamente e senza ingiustificato ritardo il Titolare e, in ogni caso, non oltre ventiquattro (24) ore dalla conoscenza della Violazione dei Dati Personali, al fine di consentire al Titolare l'adempimento degli obblighi di notifica e comunicazione previsti dagli artt. 33 e 34 del Regolamento e la rapida adozione delle possibili contromisure necessarie;

(c) collaborare con il Titolare per indagare: la natura, le categorie ed il numero approssimativo di Interessati coinvolti, le categorie ed il numero approssimativo di Dati Personali coinvolti e le probabili conseguenze di tale violazione con modalità commisurate alla serietà ed al suo impatto complessivo sul Titolare e sull'erogazione del Servizio previsto dal Contratto;

(d) ove le Leggi applicabili in materia di protezione dei Dati Personali richiedano la notificazione alle competenti Autorità di Controllo o la comunicazione agli Interessati della Violazione dei Dati Personali, e nel caso essa si riferisca a Dati Personali, il Responsabile del Trattamento dovrà deferire e assumere istruzioni dal Titolare, che – salvo quanto previsto dalla lettera a) del presente articolo - sarà l'unico ad avere il diritto di determinare le ulteriori misure che dovranno essere adottate nel rispetto delle Leggi applicabili in materia di protezione dei Dati Personali o il diritto porre rimedio a qualsivoglia rischio, tra cui ma non solo:

   i. determinare se l'avviso debba essere fornito a qualsivoglia individuo, autorità di regolamentazione, autorità giudiziaria, enti a tutela dei consumatori o altri come richiesto dalle Leggi applicabili in materia di protezione dei Dati Personali, o richiesto a discrezione del Titolare;

   ii. determinare il contenuto di tale avviso e comunicarlo ai soggetti individuati dal Titolare;

   iii. se sia possibile offrire all'Interessato dalla violazione qualsivoglia tipologia di rimedio riparatorio, nonché la natura e l'estensione di tale rimedio.

10. Trasmissione

10.1. I Dati Personali trasmessi dal Responsabile in relazione al Servizio attraverso Internet dovranno essere cifrati in modo appropriato in osservanza delle disposizioni di cui all'**Appendice 2**. Le Parti sono altresì consapevoli che la sicurezza delle trasmissioni su Internet non potrà essere completamente garantita.
10.2. In caso si sospetti una Violazione dei Dati Personali, il Responsabile potrà sospendere, immediatamente in attesa delle indagini sulle cause, l'utilizzo del Servizio via Internet da parte del Titolare, a condizione che il Responsabile notifichi tale sospensione non appena ciò sia ragionevolmente possibile, nonché adotti tutte le misure adeguate per ripristinare prontamente la fruizione del Servizio via Internet e cooperi con il Titolare al fine di proseguire l'erogazione del Servizio tramite altri canali di comunicazione disponibili.

11. Durata e validità

11.1. Il presente Accordo TDP avrà la medesima durata del Contratto di cui il presente documento costituisce un allegato. Qualora questo venisse meno o perdesse efficacia e per qualsiasi motivo, anche il presente Accordo TDP verrà automaticamente meno, senza bisogno di comunicazioni o revoche, ed il Responsabile del Trattamento non sarà più legittimato a Trattare i Dati Personali cessando lo status di Responsabile.
11.2. Con il presente Accordo TDP, il Cliente e il Responsabile intendono espressamente revocare e sostituire ogni altra eventuale nomina e accordo relativo ai medesimi prodotti per qualsivoglia tipologia di Dati Personali del Cliente.

Questo documento sostituisce integralmente e annulla il documento di nomina del 10/12/21.

Milano, 23 Maggio 2022

Per conto del Titolare (WBS):

Giovanni Pellerano

Giovanni Pellerano
Legale Rappresentante

Per conto del Responsabile (SEEWEB):

Antonio Baldassarra
Legale Rappresentante

APPENDICE 1

Categorie di interessati: i Dati Personali riguardano le seguenti categorie di Interessati: personale e collaboratori di WBS; referenti di Clienti che attivano il Servizio di Whistleblowing Digitale realizzato da WBS, soggetti riceventi le segnalazioni (Responsabili Anticorruzione, Organismi di Vigilanza, Audit, ecc.); soggetti che inviano le segnalazioni (dipendenti, collaboratori, consulenti, clienti, fornitori); Terzi indeterminati.

Tipo di Dati Personali oggetto di trattamento: i Dati Personali oggetto di trattamento si riferiscono alle seguenti tipologie di dati:

- Dati comuni: dati anagrafici, di contatto, professionali, indirizzi IP, log, ID utenti, codici di identificazione, dati bancari;
- Categorie particolari di Dati Personali: dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti allegati, relativi alla salute eventualmente contenuti nella segnalazione.

Natura e finalità del trattamento: il trattamento dei Dati Personali è obbligatorio per l'esecuzione del Servizio oggetto del Contratto.

Descrizione delle attività di trattamento: operazioni di trattamento necessarie per l'esecuzione del Servizio oggetto del Contratto.

Modalità di Trattamento

I Dati Personali sono trattati secondo modalità cartacea e elettronica.

APPENDICE 2

1. Descrizione delle misure di sicurezza tecniche ed organizzative

Il Responsabile ed i Sub-Responsabili si impegnano a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte (misure standard suggerite dallo standard ISO 27001).

2. Informazioni sulle misure di sicurezza

2.1 Gestione della sicurezza delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a definire una serie di politiche e misure per chiarire gli obiettivi al fine di supportare la sicurezza delle informazioni. A livello apicale, il Responsabile ed i Sub-Responsabili si impegnano a definire una "Policy per la sicurezza delle informazioni" di carattere generale, come specificato nella sezione 5.2 della ISO/IEC27001.

2.2 Organizzazione della sicurezza delle informazioni

2.2.1 Organizzazione interna

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'organizzazione definisca i ruoli e le responsabilità per la sicurezza delle informazioni e assegnarli singolarmente a soggetti determinati. Ove necessario, i compiti devono essere separati per ruoli e persone al fine di evitare conflitti di interesse e prevenire attività inappropriate.

2.2.2 Dispositivi mobili e telelavoro

Il Responsabile ed i Sub-Responsabili si impegnano a definire una Policy di sicurezza e adeguati controlli per i dispositivi mobili (come laptop, tablet, PC, dispositivi indossabili, smartphone, strumenti USB e altri) e per il telelavoro (come coloro che lavorano da casa, quelli che viaggiano assiduamente e le postazioni di lavoro da remoto/virtuali).

2.2.3 Sicurezza delle risorse umane

Prima dell'instaurazione del rapporto di lavoro

Il Responsabile ed i Sub-Responsabili si impegnano a prendere in considerazione le responsabilità della sicurezza delle informazioni durante l'assunzione di dipendenti, collaboratori e personale temporaneo (ad esempio attraverso adeguate descrizioni sulle mansioni da svolgere, controlli pre-assunzione) e ad inserirle all'interno dei contratti (ad

esempio con termini e condizioni del rapporto di lavoro e sottoscrizione di ulteriori accordi volti a definire ruoli e responsabilità in tema di sicurezza, obblighi di conformità, ecc.).

Durante il rapporto di lavoro

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che i manager si assicurino che i dipendenti e i collaboratori siano consapevoli e motivati a rispettare i loro obblighi per garantire la sicurezza delle informazioni. Il Responsabile ed i Sub-Responsabili si impegnano altresì a formalizzare un procedimento disciplinare per gestire gli incidenti relativi alla sicurezza delle informazioni presumibilmente causati dai lavoratori.

Conclusione o modifiche al rapporto di lavoro

Il Responsabile ed i Sub-Responsabili si impegnano a gestire gli aspetti relativi alla sicurezza al momento dell'uscita di una persona dall'organizzazione, o nelle ipotesi di modifiche significative al ruolo ricoperto, come la restituzione delle informazioni e delle apparecchiature aziendali in possesso del soggetto uscente, l'aggiornamento dei permessi di accesso, nonché il rispetto dei perduranti obblighi relativi alle informazioni riservate ed ai diritti di proprietà intellettuale, ai termini contrattuali, ecc. ed anche ai doveri etici.

2.2.4 Gestione delle risorse del patrimonio aziendale

Responsabilità delle risorse del patrimonio aziendale

Il Responsabile ed i Sub-Responsabili si impegnano a inventariare tutte le informazioni relative alle risorse del patrimonio aziendale e ad identificare i relativi soggetti di riferimento al fine di individuare le responsabilità per la loro sicurezza. Il Responsabile ed i Sub-Responsabili si impegnano altresì a definire una Policy per un "uso corretto" delle stesse e a far rientrare le risorse all'interno dell'organizzazione al momento dell'uscita dei soggetti coinvolti.

Classificazione delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a classificare e a catalogare le informazioni dai rispettivi soggetti di riferimento in linea con quanto previsto dalle esigenze di sicurezza, nonché a trattarle in modo appropriato.

Gestione dei media

Il Responsabile ed i Sub-Responsabili si impegnano a gestire, controllare, modificare ed utilizzare le informazioni conservate sui media in modo tale da non comprometterne il loro contenuto.

2.2.5 Controllo degli accessi

Requisiti aziendali per il controllo degli accessi

Il Responsabile ed i Sub-Responsabili si impegnano a documentare chiaramente i requisiti previsti dall'organizzazione per controllare l'accesso alle informazioni relative al patrimonio aziendale in una Policy per il controllo degli accessi e delle relative procedure. Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'accesso alla rete e le connessioni prevedano delle limitazioni.

Gestione dell'accesso degli utenti

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'allocazione dei diritti d'accesso da parte degli utenti sia controllata dalla registrazione iniziale dell'utente fino alla rimozione del profilo quando esso non sia più necessario, incluse speciali restrizioni per i diritti di accesso privilegiato e la gestione delle password (definita come "informazione di autenticazione segreta"); Il Responsabile ed i Sub-Responsabili si impegnano, peraltro, a procedere regolarmente alla revisione e all'aggiornamento dei diritti di accesso.

Responsabilità degli utenti

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che gli utenti siano consapevoli delle loro responsabilità attraverso il mantenimento di un effettivo controllo degli accessi, ad es. scegliendo password complesse e mantenendole riservate.

Sistemi e applicazioni per il controllo degli accessi

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'accesso alle informazioni sia limitato coerentemente a quanto previsto dalla Policy sul controllo degli accessi, ad es. attraverso autenticazioni sicure, gestione delle password, controllo delle utilità privilegiate e limitazioni all'accesso ai codici sorgente dei programmi.

2.2.6 Crittografia

Controllo crittografico

Il Responsabile ed i Sub-Responsabili si impegnano a definire una Policy sull'uso della cifratura dei dati, oltre ad autenticazioni criptate e controlli di integrità, come firme digitali e messaggi con codici di autenticazione, nonché una gestione delle chiavi di cifratura.

2.2.7 Sicurezza fisica e ambientale

Aree sicure

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che un perimetro fisico e una recinzione, con controllo fisico degli accessi e procedure operative, sia in grado di proteggere i locali, gli uffici, le stanze, le aree di carico/scarico da accessi non autorizzati. Il Responsabile ed i Sub-Responsabili si impegnano altresì a garantire la consulenza di uno specialista per quanto riguarda le misure di protezione contro incendi, allagamenti, terremoti, esplosioni, ecc.

Apparecchiatura

Il Responsabile ed i Sub-Responsabili si impegnano a rendere sicuri e manutenuti l'apparecchiatura (intesa perlopiù come apparecchiatura in ambito ICT), i servizi di supporto e il cablaggio. Il Responsabile ed i Sub-Responsabili si impegnano altresì a garantire che:

a) l'apparecchiatura e le informazioni non escano dal loro luogo di riferimento se non previa autorizzazione, e in ogni caso siano adeguatamente protette sia all'interno che all'esterno del loro luogo di riferimento;

b) le informazioni siano distrutte prima di procedere allo smaltimento o al riciclo dei dispositivi sui cui erano conservate;

c) le apparecchiature non protette siano rese sicure e sia previsto un apposito spazio ed una chiara Policy di verifica.

2.2.8 Operazioni di sicurezza

Procedure e responsabilità operative

Il Responsabile ed i Sub-Responsabili si impegnano: a documentare le procedure e le responsabilità operanti per l'area IT; a controllare i cambiamenti alle infrastrutture ed ai sistemi IT; a gestire i singoli poteri e le relative prestazioni; a separare i sistemi di sviluppo, quelli di verifica e quelli operativi.

Protezione da malware

Il Responsabile ed i Sub-Responsabili si impegnano a garantire il controllo dei malware, comprensivo di un'idonea consapevolezza sul punto da parte degli utenti.

Backup

Il Responsabile ed i Sub-Responsabili si impegnano ad eseguire Idonei backup e a custodirli coerentemente ad una Policy per i backup.

Autenticazione e monitoraggio

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che le attività, le eccezioni, gli errori e gli eventi relativi alla sicurezza delle informazioni da parte degli utenti del sistema e degli amministratori/operatori avvengano previo inserimento delle credenziali di autenticazione adeguatamente protette. Il Responsabile ed i Sub-Responsabili si impegnano altresì a garantire che gli orologi siano sincronizzati.

Controllo di software operativi

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'installazione di software sui sistemi operativi sia controllata.

Gestione delle vulnerabilità tecniche

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che le vulnerabilità tecniche siano corrette con idonee patch e che siano previste regole per l'installazione dei software da parte degli utenti.

Considerazioni sull'audit per le informazioni di sistema

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'audit per l'area IT sia programmato e controllato per minimizzare l'effetto avverso sui sistemi di produzione o l'accesso abusivo ai dati.

2.2.9 Sicurezza delle comunicazioni

Gestione della sicurezza della rete

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che le reti e i servizi in rete siano resi sicuri, ad esempio attraverso la loro separazione.

Trasferimento delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a definire policy, procedure ed accordi (ad es. accordi di riservatezza) relativi al trasferimento delle informazioni verso/da terze parti, compresi i messaggi elettronici.

2.2.10 Acquisizione, sviluppo e manutenzione del sistema

Requisiti di sicurezza dei sistemi di informazione

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che i requisiti per il controllo di sicurezza siano analizzati e specificati, comprese le applicazioni web e le transazioni.

Sicurezza nello sviluppo e processi di supporto

Il Responsabile ed i Sub-Responsabili si impegnano: a definire in una Policy le regole che governano la sicurezza dello sviluppo dei software/sistemi; a garantire che siano controllate le modifiche al sistema (sia per le applicazioni che per i sistemi operativi); a garantire che i pacchetti software non siano teoricamente modificati e che siano osservati i principi di sicurezza ingegneristica; a rendere sicuro l'ambiente di sviluppo e controllare lo sviluppo esternalizzato; a garantire che la sicurezza del sistema sia testata e che siano definiti criteri di ammissibilità che includano gli aspetti di sicurezza.

Test di verifica dei dati

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che i test di verifica dei dati siano accuratamente selezionati/generati e controllati.

2.2.11 Rapporti con i fornitori

Sicurezza delle informazioni nei rapporti coi fornitori

Il Responsabile ed i Sub-Responsabili si impegnano a definire policy, procedure, sistemi di consapevolezza volti a proteggere le informazioni dell'organizzazione che siano accessibili ai soggetti esterni operanti nell'area IT e ad altri fornitori esterni per l'intera catena di fornitura, concordata nei contratti o negli accordi.

Gestione dei servizi resi dal fornitore

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'erogazione dei servizi resi dal fornitore sia monitorata e rivista/verificata in relazione al contratto/accordo e che le modifiche al servizio siano controllate.

2.2.12 Gestione degli incidenti alle informazioni di sicurezza

Gestione degli incidenti alle informazioni di sicurezza e miglioramenti

Dovrebbero essere previste responsabilità e procedure (report, valutazioni, rispondere a e imparare da) volte a gestire in modo coerente ed efficace gli eventi, gli incidenti e le debolezze relative alle informazioni di sicurezza, anche al fine di conservare prove valide in eventuali giudizi.

2.2.13 Aspetti della sicurezza delle informazioni relativi alla continuità aziendale

Continuità della sicurezza delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che la continuità della sicurezza delle informazioni sia pianificata, implementata e revisionata come parte integrante del sistema organizzativo di continuità aziendale.

Ridondanze

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che le strutture IT siano sufficientemente ridondanti per soddisfare i requisiti di disponibilità.

2.2.14 Conformità

Conformità ai requisiti legali e contrattuali

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'organizzazione identifichi e documenti i suoi obblighi alle autorità esterne e ad altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile, le informazioni relative alla privacy/comunque idonee a consentire l'identificazione personale e la crittografia.

Revisione della sicurezza delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che i progetti dell'organizzazione relativamente alla sicurezza delle informazioni siano revisionati (verificati tramite audit) con modalità tali da garantire l'indipendenza della valutazione e rendicontate alla Direzione. Il Responsabile ed i Sub-Responsabili si impegnano altresì a garantire che i manager revisionino periodicamente la conformità dei dipendenti e dei sistemi alle policy di sicurezza, alle procedure, ecc., e promuovano azioni correttive ove necessario.

APPENDICE 3

(Elenco dei Sub-Responsabili)

La tabella dei Sub-Responsabili deve essere compilata di volta in volta da SEEWEB e trasmessa a WS in modo che WBS possa opporsi all'impiego di nuovi Sub-Responsabili ai sensi dell'art. 28 del Regolamento.

Sub-Responsabili (indicare: luogo di stabilimento e dettagli di contatto) *Ad es., Nome della società, Indirizzo, soggetto responsabile in materia di protezione dei Dati Personali e dettagli di contatto*	**Paese/i in cui i Dati Personali sono trattati e finalità** *Ad es., Italia per hosting e Francia per backup*
non previsti	

CISQ is a member of

IQNET

The International Certification Network

www.iqnet-certification.com

CERTIFICATO n°
CERTIFICATE n° **50030**

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

WHISTLEBLOWING SOLUTIONS IMPRESA SOCIALE S.r.l.

IT - 20131 MILANO (MI) - VIALE ABRUZZI 13/A

NELLE SEGUENTI UNITA' OPERATIVE / IN THE FOLLOWING OPERATIVE UNITS

IT - 20131 MILANO (MI) - VIALE ABRUZZI 13/A

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**

Servizi di ricerca, sviluppo e progettazione di infrastrutture tecnologicamente innovative di whistleblowing sicuro ed erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks.
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 31/01/2023.

Research, development and design services of technologically innovative infrastructures of safe whistleblowing and provision of Saas services of Digital Whistleblowing based on GlobaLeaks.
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 31/01/2023.

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*	*09/03/2023*
DATA SCADENZA *EXPIRY DATE*	*11/03/2026*
EMISSIONE CORRENTE *CURRENT ISSUE*	*09/03/2023*

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

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

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

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.

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.

C02 ED 03 151122

CONFORMITÀ AL PRINCIPIO DNSH (DO NOT SIGNIFICATIVE HARM)

Premessa

Oggi le amministrazioni devono andare nella direzione di scelte e misure che dimostrino di non arrecare danni significativi all'ambiente e ai nuovi target ambientali.
In particolare, secondo il Dispositivo per la ripresa e la resilienza (Regolamento UE 241/2021), tutte le misure dei Piani nazionali (PNRR) devono soddisfare il principio di "non arrecare danno significativo agli obiettivi ambientali". Tale vincolo si traduce in una valutazione di conformità degli interventi al principio del **"Do No Significant Harm" (DNSH)**, il cui obiettivo è valutare se una misura possa o meno arrecare un danno ai sei obiettivi ambientali individuati nel Green Deal europeo.

DNSH e Data Center

Il contesto attuale vede le amministrazioni chiamate ad accelerare i processi di digitalizzazione e, contestualmente, a investire in modo sostenibile, coerentemente con quanto riportato nelle valutazioni DNSH.
E se i data center sono luoghi di erogazione di servizi indispensabili per la trasformazione digitale, è vero anche che sono estremamente energivori: è quindi necessario che siano progettati in modo da contribuire al massimo agli obiettivi di miglioramento climatico.

Conformità di Whistleblowing Solutions Impresa Sociale al principio DNSH

Al fine di attestare il possesso dei requisiti ambientali DNSH (Do No Significant Harm), Whistleblowing Solutions Impresa Sociale, impegnata sin dalla sua nascita nel monitoraggio delle emissioni e nella scelta di processi sostenibili, dichiara di:

- non arrecare danno significativo all'ambiente;
- selezionare solo fornitori con certificazione ambientale ISO14001;

Il fornitore IaaS selezionato è Seeweb S.r.l. Il quale:

- dispone di certificazione ambientale ISO14001 ed è impegnato per l'acquisto di ogni nuova apparecchiatura IT a selezionare solo apparecchiature certificate secondo lo standard internazionale sull'efficienza energetica Energy Star, o equivalente secondo le norme EPA ENERGY STAR - ISO 30134-4:2017;
- dichiara che le nuove apparecchiature IT acquisite sono certificate secondo lo standard internazionale sull'efficienza energetica Energy Star, o equivalente, secondo le norme EPA ENERGY STAR - ISO/IEC 30134-4:2017;
- dispone di datacenter che prevedono un piano di gestione dei rifiuti in linea con la norma LCA - EN50625;
- dispone della certificazione che attesta che i refrigeranti utilizzati nei sistemi di raffreddamento dei data center sono conformi al Regolamento (EU) n. 517/204 del

Parlamento Europeo e del consiglio del 16 aprile 2014 sui gas fluorurati a effetto serra, che abroga il regolamento (CE) n.842/2006;

- dispone della certificazione delle apparecchiature dei data center in conformità con la direttiva sulla restrizione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche (EU) 2011/65.
- dichiara in aggiunta a quanto previsto da DNSH l'impegno a usare solo energia certificata rinnovabile per l'alimentazione dei suoi data center.

Milano, 19 maggio 2022

_____

Luogo e data

Giovanni Pellerano

Whistleblowing Solutions Impresa Sociale S.r.l.
Legale Rappresentante
Giovanni Pellerano

INFORMATIVA IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI
ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679
IN RELAZIONE ALLE SEGNALAZIONI DI "WHISTLEBLOWING"

Con questa informativa l'Amministrazione provinciale di Terni spiega come tratta i dati raccolti e quali sono i diritti riconosciuti all'interessato ai sensi del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e del d.lgs. 196/2003, in materia di protezione dei dati personali, così come modificato dal d.lgs. 101/2018.

1. Titolare del trattamento

Titolare del trattamento dei dati personali è l'Amministrazione provinciale di Terni, avente sede in Viale della Stazione 1, 05100 Terni TR - Telefono: +39 0744 4831 - Fax: +39 0744 483250 - Partita IVA: 00179350558 - PEC: provincia.terni@postacert.umbria.it

2. Responsabile della protezione dati

Il Responsabile della protezione dati è il Dott. Giuliano Palotto (quale referente di Unica Società Cooperativa) nominato con Decreto del Presidente della Provincia n. 1234 del 19/01/2023.
Il dato di contatto del Responsabile della protezione dati è: dpo@provincia.terni.it

3. Finalità del trattamento

I dati da lei direttamente forniti per segnalare, nell'interesse dell'integrità della Pubblica Amministrazione, presunte condotte illecite delle quali sia venuto a conoscenza in ragione del proprio rapporto di lavoro, servizio o fornitura con l'Agenzia delle entrate, verranno trattati dall'Amministrazione stessa per gestire tali situazioni. I dati personali sono dunque acquisiti in quanto contenuti nella segnalazione e/o in atti e documenti a questa allegati, si riferiscono al soggetto segnalante e possono altresì riferirsi a persone indicate come possibili responsabili delle condotte illecite, nonché a quelle a vario titolo coinvolte nelle vicende segnalate. In particolare, per svolgere le necessarie attività istruttorie volte a verificare la fondatezza di quanto segnalato, nonché, se del caso, adottare adeguate misure correttive e intraprendere le opportune azioni disciplinari e/o giudiziarie nei confronti dei responsabili delle condotte illecite.

4. Tipologia di dati trattati

La ricezione e la gestione delle segnalazioni dà luogo a trattamenti di dati personali c.d. "comuni" (nome, cognome, ruolo lavorativo, ecc.), nonché può dar luogo, a seconda del contenuto delle segnalazioni e degli atti e documenti a queste allegati, a trattamenti di dati personali c.d. "particolari" (dati relativi a condizioni di salute, orientamento sessuale o appartenenza sindacale, di cui all'art. 9 GDPR) e di dati personali relativi a condanne penali e reati (di cui all'art. 10 GDPR).

5. Basi giuridiche del trattamento

Tenuto conto della normativa di riferimento e, in particolare, dell'art. 54-bis D.lgs. 165/2001, si precisa che:

- il trattamento dei dati "comuni" si fonda sull'obbligo di legge a cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c) del GDPR), nonché sull'esecuzione di compiti di interesse pubblico assegnati dalla legge all'Amministrazione provinciale di Terni (art. 6, par. 1, lett. e) del GDPR);
- il trattamento di dati "particolari" si fonda sull'assolvimento di obblighi e sull'esercizio di diritti specifici del Titolare del trattamento e dell'Interessato in materia di diritto del lavoro (art. 9, par. 2, lett. b), GDPR), nonché sull'esecuzione di un compito di interesse pubblico

rilevante assegnato dalla legge all'Amministrazione provinciale di Terni (art. 9, par. 2, lett. g), GDPR), in ragione dell'art. 2-sexies lett. dd) del D.lgs.196/2003;

- il trattamento di dati relativi a condanne penali e reati, tenuto conto di quanto disposto dall'art. 10 GDPR, si fonda sull'obbligo di legge a cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c), GDPR) e sull'esecuzione di compiti di interesse pubblico assegnati dalla legge all'Amministrazione provinciale di Terni (art. 6, par. 1, lett. e), GDPR), in ragione dell'art. 2-octies lett. a) del D.lgs. 196/2003. Si precisa che, in ragione di quanto disposto dall'art. 54-bis D.lgs. 165/2001, nel caso in cui la segnalazione portasse all'instaurazione di un procedimento disciplinare nei confronti del responsabile della condotta illecita, l'identità del segnalante non verrà mai rivelata.

Qualora la conoscenza dell'identità del segnalante fosse indispensabile per la difesa dell'incolpato, verrà domandato al segnalante se intende rilasciare un apposito, libero consenso ai fini della rivelazione della propria identità; in caso di mancato consenso, il procedimento disciplinare verrà archiviato.

6. Soggetti autorizzati a trattare i dati

A sua tutela, solo il Responsabile della prevenzione della corruzione e della trasparenza (RPCT), all'interno della Provincia di Terni, è in grado di associare le segnalazioni alle identità dei segnalanti. Il RPCT è il Segretario Generale dell'Ente; in caso di sua assenza o impedimento è il Vice Segretario dell'Ente. Qualora esigenze istruttorie richiedano che altri soggetti, all'interno della Provincia di Terni, debbano essere messi a conoscenza del contenuto della segnalazione o della documentazione ad essa allegata, non verrà mai rivelata l'identità del segnalante, né verranno rivelati elementi che possano, anche indirettamente, consentire l'identificazione dello stesso. Tali soggetti, poiché potrebbero comunque venire a conoscenza di altri dati personali, sono comunque tutti formalmente autorizzati al trattamento e a ciò appositamente istruiti e formati, nonché tenuti a mantenere il segreto su quanto appreso in ragione delle proprie mansioni, fatti salvi gli obblighi di segnalazione e di denuncia di cui all'art. 331 del Codice di procedura penale.

7. Responsabile del trattamento

L'Amministrazione provinciale di Terni si avvale di società esterna, in qualità di partner tecnologico, per la gestione della piattaforma utilizzata, designata per questo Responsabile del trattamento dei dati ai sensi dell'art. 28 del Regolamento (UE) 2016/679.

8. Categorie di destinatari dei dati personali

I suoi dati personali e quelli delle persone indicate come possibili responsabili delle condotte illecite, nonché delle persone a vario titolo coinvolte nelle vicende segnalate, non saranno oggetto di diffusione, tuttavia, se necessario, su loro richiesta, possono essere trasmessi all'Autorità Giudiziaria, alla Corte dei conti e all'ANAC, Autorità nazionale anticorruzione. Tali soggetti sono, tutti, Titolari autonomi del trattamento. Alla segnalazione e all'identità del segnalante non è possibile accedere né a mezzo accesso documentale, né a mezzo accesso civico generalizzato. Nell'ambito dei procedimenti penali eventualmente istaurati, l'identità del segnalante sarà coperta da segreto nei modi e nei limiti previsti dall'art. 329 c.p.p.; nell'ambito di procedimenti dinanzi alla Corte dei conti, l'identità del segnalante non sarà comunque rivelata sino alla chiusura della fase istruttoria; nell'ambito dei procedimenti disciplinari, l'identità del segnalante non sarà rivelata in tutti i casi in cui la contestazione dell'addebito disciplinare si fondi su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa, mentre potrà essere rivelata laddove concorrano, insieme, tre presupposti, ovverosia (a) che la contestazione si fondi, in tutto o in parte, sulla segnalazione, (b) che la conoscenza dell'identità del segnalante sia indispensabile per

la difesa dell'incolpato e che (c) il segnalante abbia espresso un apposito consenso alla rivelazione della propria identità.

9. Modalità del trattamento

I dati personali saranno trattati anche con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. L'Amministrazione provinciale di Terni attua idonee misure per garantire che i dati forniti vengano trattati in modo adeguato e conforme alle finalità per cui vengono gestiti; l'Amministrazione provinciale di Terni impiega idonee misure di sicurezza (crittografia dei file), organizzative, tecniche e fisiche, per tutelare le informazioni dall'alterazione, dalla distruzione, dalla perdita, dal furto o dall'utilizzo improprio o illegittimo.

10. Periodo di conservazione dei dati

Il RPCT effettua un'attività istruttoria preliminare della segnalazione. Se a seguito dell'attività svolta ravvisa elementi di manifesta infondatezza ne dispone l'archiviazione. Nel caso, invece, il RPCT ravvisi il fumus di fondatezza della segnalazione, trasmette la stessa, priva dei dati del segnalante, agli organi preposti interni o esterni, ognuno secondo le proprie competenze. I dati personali vengono conservati per un periodo di 18 mesi e, comunque, sino alla definizione dei procedimenti avviati dagli uffici o dagli Enti destinatari della segnalazione.

11. Natura del conferimento dei dati e conseguenze dell'eventuale mancato conferimento

Al fine di classificare la segnalazione come whistleblowing i suoi dati identificativi (nome, cognome) devono essere forniti obbligatoriamente in quanto, come precisato da ANAC (Autorità Nazionale Anticorruzione), le segnalazioni anonime non rientrano direttamente nel campo di applicazione dell'art. 54 bis del d.lgs. 165/2001. Nel caso in cui il segnalante volesse comunque procedere con segnalazione anonima, quest'ultima verrà gestita con modalità ordinarie; tale segnalazione verrà presa in considerazione esclusivamente laddove adeguatamente circostanziata, resa con dovizia di particolari e dunque in grado di far emergere fatti e situazioni relazionandoli a contesti determinati. E' rimessa invece a ciascun segnalante la decisione circa quali ulteriori dati personali conferire. Maggiori sono i dettagli presenti nella segnalazione, maggiori saranno le possibilità per l'Amministrazione provinciale di Terni di intervenire nell'interesse dell'integrità della Pubblica Amministrazione.

12. Diritti

Lei ha il diritto, in qualunque momento, di ottenere la conferma dell'esistenza o meno dei dati forniti. Ha inoltre il diritto di chiedere, nelle forme previste dall'ordinamento, la rettifica dei dati personali inesatti e l'integrazione di quelli incompleti e di esercitare ogni altro diritto ai sensi degli articoli da 18 a 22 del Regolamento laddove applicabili. Nel caso abbia dato il consenso alla rivelazione della sua identità nell'ambito di procedmenti disciplinari, ha il diritto di revocare tale consenso in qualsiasi momento, senza che però ciò pregiudichi la liceità del trattamento, basato sul consenso, effettuato prima della revoca. Tali diritti possono essere esercitati con richiesta indirizzata al Titolare del trattamento ai recapiti indicati al punto 1 della presente. Qualora ritenga che il trattamento sia avvenuto in modo non conforme al Regolamento e al d.lgs. 196/2003, potrà rivolgersi al Garante per la Protezione dei dati Personali, ai sensi dell'art. 77 del medesimo Regolamento. Ulteriori informazioni in ordine ai suoi diritti sulla protezione dei dati personali sono reperibili sul sito web del Garante per la Protezione dei Dati Personali all'indirizzo www.garanteprivacy.it.