Valutazione di Impatto o
Data Protection Impact Assessment
Processo di Gestione del Whistleblowing

Comune di Arcene
Provincia di Bergamo

1 Premessa

Il regolamento europeo sul trattamento dei dati impone al titolare di attuare delle azioni per la protezione delle informazioni e per l'applicazione dei diritti degli interessati. Il trattamento dei dati ha maggiori livelli di rischio quando si attua un monitoraggio sistemico dei comportamenti degli interessati, o per il gran numero dei soggetti coinvolti, le tecnologie utilizzate di cui sono magari trattati dati personali particolari, o anche per una combinazione di questi e altri fattori.
Tra le procedure che il Titolare deve attuare rientra quanto previsto all'art. 35 del GDPR, che prevede una valutazione preventiva dell'impatto dei trattamenti previsti sulla protezione dei dati, anche in considerazione di possibili rischi per i diritti e le libertà delle persone fisiche (di seguito, "DPIA").
La Valutazione d'Impatto sulla Protezione dei Dati 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.
La DPIA è un processo dinamico, che ha l'obiettivo di verificare il livello di rischio, e di attuazione dei diritti degli interessati derivanti dal trattamento dei dati e di identificare eventuali azioni per ridurre il rischio stesso.

2 Obiettivo del documento

Il presente documento ha l'obiettivo di descrivere il processo metodologico con cui viene effettuata la DPIA svolta dal Comune di Arcene, i risultati della stessa in relazione ai trattamenti concernenti l'attivazione delle segnalazioni di illeciti identificati dal D. Lgs. 24/2023 (disciplina sul whistleblowing).
Attraverso l'analisi verranno identificate le misure tecniche, organizzative e procedurali da adottare per un corretto trattamento dei dati e il contenimento dei livelli di rischi insiti nel processo di trattamento in seguito alle misure di protezione adottate. Nel caso in cui il risultato della valutazione di Impatto presenti un rischio elevato prima di attuare il trattamento deve essere fatta consultazione preventiva con l'autorità garante della protezione dei dati.

3 Normativa di riferimento

- **Regolamento UE n. 2016/679** 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;
- **Art 35 del GDPR:** 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.
- **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 4 aprile 2017 (versione successivamente emendata e adottata il 4 ottobre 2017).
- **D.Lgs. 30 giugno 2003, n, 196,** recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;
- **Legge 190/2012** "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione",
- **D.Lgs. n. 165/2001**, "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", introduce l'articolo 54-bis, intitolato "Tutela del dipendente pubblico che segnala illeciti".
- **Legge 179/2017 sul Whistleblowing** approvata il 15/11/2017 a tutela del dipendente pubblico e privato, che prevede che sia predisposto "almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante".

- Regolamento ANAC del 01 luglio 2020 per la gestione delle segnalazioni e per l'esercizio del potere sanzionatorio in materia di tutela degli autori di segnalazioni di illeciti o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui all'art. 54 bis Decreto legislativo n. 165/2001.
- PNA (Piano Nazionale Anticorruzione) 2019 Delibera ANAC n. 1064 del 13 novembre 2019: Il RPCT, oltre a ricevere e prendere in carico le segnalazioni, pone in essere gli atti necessari ad una prima attività di verifica e di analisi delle segnalazioni ricevute da ritenersi obbligatoria in base al co. 6 dell'art. 54-bis
- **Delibera ANAC n. 469 del 9 giugno 2021 L'ANAC**, che contiene le "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)", con la chiara indicazione che le segnalazioni, al fine di tutelare il segnalante, debbano essere trattate con sistemi informatizzati e crittografici.
- **D. Lgs. 24/2023** Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

4 Definizioni

Dato personale: 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;

Dato Personale Particolare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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."

Probabilità: valutazione della frequenza di accadimento di un evento, in funzione di eventi esterni non determinabili, delle vulnerabilità in essere e di eventuali contromisure implementate.

Impatto: indicazione del livello di incidenza di un evento che può compromettere la riservatezza, l'integrità e la disponibilità dei dati e dei diritti degli interessati;

Minaccia: evento potenziale, accidentale o deliberato, che, nel caso accadesse, produrrebbe un danno per l'interessato;

Vulnerabilità: debolezza intrinseca del sistema di gestione del dato che, qualora si realizzasse una minaccia, produrrebbe un danno all'interessato;

Rischio: è uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà. Il rischio in questa procedura è sempre riferito all'interessato

Contromisure: interventi tecnologici, procedure organizzative che possono essere implementate al fine di mitigare il Rischio Privacy associato ad ogni sistema o archivio e quindi diminuire il Rischio;

DPIA: data protection impact assessment

RPCT: Responsabile della prevenzione della corruzione e della trasparenza
RPCT: Responsabile della prevenzione della corruzione e della trasparenza

Whistleblowing: in questo ambito si intende la disciplina che ha recepito la Direttiva UE 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

ACN: Agenzia di cybersecurity nazionale https://www.acn.gov.it/

5 Campo di Applicazione

La presente analisi si applica al trattamento dei dati relativi al processo di whistleblowing attivato dal Comune di Arcene.

6 Compiti e responsabilità

Titolare dei trattamenti
La responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare ne monitora lo svolgimento consultandosi con il responsabile della protezione dei dati (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore.

Amministratore di sistema Informativo
Partecipa al processo di valutazione dei rischi e alla attuazione delle contromisure per il contenimento dei rischi.

Responsabile della protezione dei Dati
Supporta il titolare nell'analisi del processo di trattamento dei dati e nella valutazione della corretta attuazione degli adempimenti e delle misure di sicurezza per la protezione dei diritti degli interessati.
Il responsabile della protezione dei dati, fornisce un parere in merito alla valutazione di impatto.
Valuta inoltre i passi da intraprendere per la comunicazione all'autorità garante della protezione dei dati se il risultato della valutazione di impatto rileva un livello di rischio elevato per i dati degli interessati.

Componente del Team di Lavoro
La valutazione di impatto può richiedere la partecipazione di esperti dei processi di trattamento e della tecnologia utilizzata. Il soggetto in questione può essere sia un soggetto interno all'organizzazione o un soggetto esterno. Lo stesso è tenuto a fornire un apporto alla conduzione della DPIA nelle varie fasi.

7 Descrizione del contesto relativo al trattamento dei dati

Il comune di Arcene in ottemperanza alla **Legge 179/2017 sul Whistleblowing e al D. Lgs. 24/2023** Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo ha avviato un'attività di adeguamento del processo di gestione delle segnalazioni che tiene conto anche dei recenti provvedimenti adottati dall'ANAC.
A tal fine l'ente ha valutato di dotarsi di una piattaforma applicativa che consenta di gestire il processo di segnalazione di illeciti e che rispetti le disposizioni dell'Autorità Nazionale per l'Anti Corruzione.
L'analisi effettuata ha considerato la soluzione applicativa sviluppata da Whistleblowing Solutions I.S. S.r.l., di cui si allega il documento rilasciato dal fornitore che ne descrive le caratteristiche tecniche ed infrastrutturali.

8 Attività di trattamento

DESCRIZIONE DELL'ATTIVITA' DI TRATTAMENTO	
Titolare del trattamento	Comune di Arcene
Contitolare del trattamento	Non presente
Area che gestisce il trattamento	Responsabile dell'anticorruzione del Comune nella persona del segretario comunale Dott.ssa Mariarosa Armanni
Settore/ufficio	Responsabile dell'anticorruzione del Comune nella persona del segretario comunale Dott.ssa Mariarosa Armanni
Altri soggetti che accedono alla banca dati	Nessun soggetto accede ai dati della piattaforma che sono salvati in modalità cifrata
Incaricati al trattamento	Non sono previsti soggetti autorizzati al trattamento se non il responsabile dell'anticorruzione
Soggetto terzo qualificato come responsabile del trattamento	Whistleblowing Solutions che fornisce la piattaforma applicativa in modalità SAAS e gestisce la manutenzione della piattaforma applicativa
Soggetto terzo qualificato come sub-responsabile del trattamento	**Seeweb** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS) **Transparency International Italia** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing
DPO	Luigi Mangili 800 121 961 dpo-arcene@cloudassistance.it
Descrizione del trattamento	
Finalità del trattamento	Attivazione piattaforma applicativa per la gestione del processo di whistleblowing in modalità digitale incluse le attività di segnalazione di i reati o irregolarità di cui siano venuti a conoscenza i dipendenti dell'ente in ragione di un rapporto di lavoro fornitori e stakeholder in generale.
Base giuridica del trattamento	Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
Tipologia di dati trattati	Dati personali dei soggetti che segnalano delle irregolarità Dati relativi alla segnalazione della presunta violazione normativa in materia di gestione degli appalti
Categorie degli interessati	dipendenti che segnalano reati o irregolarità, fornitori, amministratori, stakeholder in generale
Perimetro in cui i dati sono trattati	I dati vengono trattati nell'ambito del processo di gestione delle segnalazioni di irregolarità dei diritti dell'unione nella gestione dei procedimenti organizzativi dell'ente identificati dal D Lgs 24/2023.
Modalità di trattamento	I dati vengono trattati in formato digitale, attraverso la piattaforma applicativa di whistleblowing che gestisce i processi di comunicazione e salvataggio dei dati in modalità cifrata. 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.
Tempi di conservazione dei dati	I dati sono trattati per un periodo necessario per gestire le attività di accertamento e di istruttoria in seguito alla segnalazione di reati o irregolarità. Al termine del contratto di utilizzo della piattaforma e alla scadenza degli obblighi di legge per finalità amministrative e contabili viene predisposta la conseguente cancellazione sicura dei dati da parte del fornitore
Destinatari a cui i dati sono comunicati	ANAC Autorità giudiziaria Altri soggetti nel rispetto della normativa di legge
Diffusione dei dati	I dati non sono soggetti a diffusione
Valutazione della necessità e della proporzionalità del trattamento	
Necessità e proporzionalità del trattamento.	Al fine di rendere efficace e di digitalizzare il processo di whistleblowing il Comune di Arcene intende adottare la piattaforma applicativa sviluppata Whistleblowing Solution.
È stata effettuata una consultazione preventiva con gli interessati al trattamento	Le caratteristiche del processo di trattamento non prevedono la consultazione preventiva degli interessati
Asset usati per il trattamento	
Luoghi fisici	La piattaforma applicativa viene erogata in modalità SAAS ed è installata presso provider identificato dal fornitore della soluzione applicativa.
Hardware	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	La piattaforma informatica di segnalazione è basata sul software GlobaLeaks1. 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 Nel caso di segnalazione che pervengono in altre modalità il responsabile dell'anticorruzione dispone di una cartella su server sulla quale vengono salvati i dati relativi all'istruttoria protetti da password.
Reti di comunicazione	Le reti di trasmissioni dei dati usano protocolli sicuri di cifratura
Possibilità accesso remoto	Non è prevista questa modalità di accesso da parte di soggetti terzi L'applicativo è una piattaforma web accessibile attraverso browser in modalità SAAS.
Diritti degli interessati	
Come sono stati informati gli interessati	Il titolare ha predisposto una informativa nella quale sono indicate le policy relative al trattamento dei dati.
Accesso ai dati	L'accesso ai dati è consentito solo al soggetto interessato che effettua la segnalazione e al responsabile dell'anticorruzione
Rettifica dei dati	La rettifica dei dati è consentita solo al soggetto interessato che effettua la

	segnalazione
Cancellazione	I dati vengono cancellati al termine dell'iter di gestione del procedimento nel rispetto della normativa di legge.
Portabilità	Diritto non previsto per il tipo di trattamento
Opposizione	L'inserimento dei dati per segnalazione di un illecito è su base volontaria per cui questo principio non si applica
Limitazione di trattamento	I dati vengono trattati per un tempo limitato come indicato nell'informativa
Revoca del consenso	Il trattamento non si basa sul consenso al trattamento dei dati ma costituisce un libero arbitrio del soggetto procedere alla segnalazione di un illecito
Limitazione della finalità	I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità L'accesso ai dati è regolamentato e consentito solo al responsabile dell'anticorruzione Le finalità sono rese note all'interno nell'informativa relative al trattamento dei dati
Limitazione della conservazione	I dati sono conservati in modalità cifrata che non consente l'identificazione degli interessati se non ai soggetti autorizzati al trattamento. Il tempo di conservazione rispetta le disposizioni normative e procedurali definite da ANAC
Integrità e riservatezza	La piattaforma applicativa adotta misure di sicurezza tecnologiche per la protezione dei dati quali ● Registrazione delle operazioni eseguite in file di log che non prevedono l'identificazione dei soggetti che hanno fatto la segnalazione; ● Protezione degli apparati di elaborazione; ● Cifratura dei dati registrati; ● Utilizzo prettamente di piattaforme open source
Coinvolgimento del DPO	Il DPO nominato dall'ente è stato consultato sulla redazione della DPIA

9 VALUTAZIONE DEI RISCHI PER DIRITTI E LIBERTÀ E PER LA PROTEZIONE DEI DATI DEGLI INTERESSATI

La valutazione del rischio è il processo complessivo di: identificazione del rischio, analisi del rischio e accertamento (in senso stretto) del rischio. I rischi possono essere valutati a livello di organizzazione, di dipartimento, per singoli trattamenti, per processi o attività individuali o per rischi specifici.
La valutazione del rischio fornisce una comprensione delle loro cause, delle conseguenze e connesse probabilità. Ciò costituisce l'input a decisioni del tipo:

- se l'attività di trattamento deve essere intrapresa, o no
- se i rischi devono essere trattati - scegliere tra opzioni con rischi differenti
- mettere in priorità le opzioni di trattamento dei rischi (riduzione, trasferimento, accettazione e monitoraggio).
- selezionare le strategie più appropriate per il trattamento degli stessi, che possono condurre ad un livello tollerabile.

Per fornire una misurazione sul livello di rischio a cui l'organizzazione va incontro si utilizza un metodo **quantitativo** per valutare l'indice di rischio attraverso una valutazione legata a diversi parametri

Le definizioni applicate ai fini dell'analisi dei rischi sono:

Probabilità: frequenza del verificarsi delle conseguenze;
Impatto: qualunque conseguenza negativa derivante dal verificarsi dell'evento;
Indice Rischio (ID): combinazione della probabilità di accadimento di un danno e della gravità di quel danno.
Per misurare il rischio l'ente utilizza la relazione:

R: P x D e le seguenti scale:

Criteri per determinare la probabilità di accadimento		
P	Livello di probabilità	Criteri di valutazione
4	Alta	Accade di frequente
3	Media	Può accadere diverse volte
2	Bassa	Può accadere talvolta
1	trascurabile	Improbabile

Criteri per determinare l'Impatto		
P	Livello di probabilità	Criteri di valutazione
4	Alta	Grave danno per i diritti e le libertà degli interessati
3	Media	danno Medio per i diritti e le libertà degli interessati
2	Bassa	danno Basso per i diritti e le libertà degli interessati
1	trascurabile	danno Trascurabile

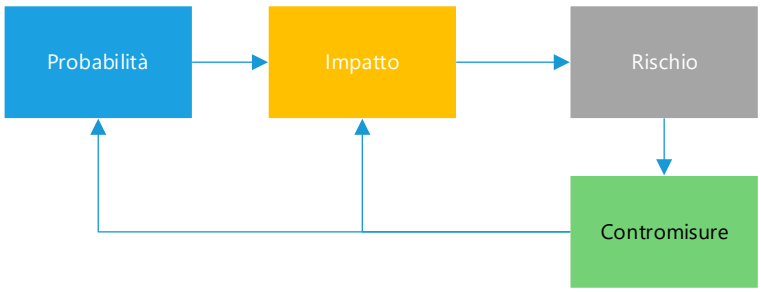
Il comune ha sviluppato questa attività ed ha sintetizzato il risultato di questo lavoro nella matrice di seguito allegata.

Probabilità					
	IR	1	2	3	4
danno	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

	Rischio basso		Rischio medio		Rischio alto		Rischio altissimo
	Monitorare		Monitorare		Azione Correttiva o piano di Miglioramento		Azione Correttiva

Nel caso in cui il rischio relativo ad un'attività di trattamento sia alto o altissimo si deve procedere con una mitigazione dello stesso adottando un'azione per il contenimento e valutare in seguito l'esito di questa azione in termini di indice di rischio.

Metodo valutazione del Rischio



10 Valutazione di impatto

Nella tabella di seguito riportata sono riportati gli esiti della valutazione di impatto
La valutazione di impatto analizza la piattaforma applicativa utilizzata per la gestione delle segnalazioni ma anche il sistema informativo del comune in quanto le segnalazioni pervenute al RPTC vengono poi trattate con dispositivi informatici che devono in ogni caso garantire la riservatezza del dato di che ha effettuato la segnalazione.

10.1 Misure di Sicurezza attivate

Di seguito vengono descritte le misure di sicurezza adottate dall'ente per la protezione dei dati Trattandosi di un servizio applicativo parte delle misure di sicurezza vengono gestite dal fornitore dell'applicazione, ma parte del trattamento dei dati viene eseguito nel perimetro della sede dell'ente e del sistema informativo comunale, motivo per cui nell'analisi dei rischi si fa riferimento anche a questi aspetti.

Misure sicurezza edificio
Accessi tramite porta vetri struttura in alluminio dotati di chiave di sicurezza
Allarme volumetrico
Sistema antincendio costituito da estintori manutenuti da una ditta specializzata
Sistema di rilevazione degli incendi
Misure sicurezza Data Center ed infrastruttura di rete su cui è installata la piattaforma di whistleblowing
La soluzione applicativa è installata su data center certificato ACN
Un cluster di due firewall perimetrali;
Un cluster di due server fisici dedicati;
Una storage area network pienamente ridondata.
Misure sicurezza adottate dalla Piattaforma Applicativa di whistleblowing
Dati salvati in modalità cifrata
Registrazione dei log anonimizzata
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;
VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definite insieme di amministratori di sistema;
Tutti i dispositivi utilizzati quali applicativo WhistleblowingPA che si basa sulla piattaforma 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 indirizzi IP e User Agents
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.
Misure sicurezza sala server dell'ente
Accesso al solo personale autorizzato tramite porta chiusa a chiave
Estintori installati localmente
Climatizzazione della sala server
Misure sicurezza organizzative
Nomina del responsabile dell'anticorruzione
Approvazione di una linea guida relativa alla protezione dei dati
Misure sicurezza tecnologica dell'ente
Server alimentati con batterie di continuità
Impianto elettrico a norma
Cartelle in cui vengono eventualmente conservate le registrazioni profilate, ed autorizzazioni di accesso ai soli incaricati
Protezione del server tramite tools di sicurezza ed antivirus
Protezione delle postazioni di lavoro tramite tools di sicurezza ed antivirus
Protezione della rete tramite apparati perimetrali (firewall)
Vengono fatte delle copie di sicurezza delle cartelle del server nel quale sono eventualmente conservate i

dati e l’istruttoria relativa alle segnalazioni relative al processo di whistleblowing

Di seguito viene riportato lo schema con cui viene effettuata l’analisi dei rischi in materia di trattamento dei dati avente come elemento di protezione i dati ed i diritti dell’interessato.

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Non rispetto diritti degli interessati							
Furto di dati	Violazione delle libertà o della dignità per l'interessato	1	3	3	Accesso ai dati è consentito solo a personale autorizzato a cui è associato un profilo di accesso ai dati in funzione della mansione attribuita (Responsabile anticorruzione). Il comune ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati Il fornitore della piattaforma applicativa ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati come descritto nella documentazione tecnica fornita		
Rischio che gli interessati possano essere non adeguatamente informati sul trattamento dei loro dati	Reclami degli interessati Violazione delle libertà	2	1	2	L'ente ha predisposto una informativa sul trattamento dei dati che è stata pubblicata sul sito istituzionale del comune		
Rischi che i dati possano essere utilizzati non rispettando i limiti delle finalità per cui sono raccolti o che vengano raccolti dati eccedenti le finalità previste dal progetto.	Reclami degli interessati	1	2	2	I dati vengono raccolti per finalità legittime in base alle norme di legge in materia di whistleblowing. Il tempo di conservazioni rispetta le finalità del trattamento inerenti la gestione della segnalazione e la necessità di gestire l'istruttoria I dati vengono forniti volontariamente dall'interessato L'ente ha predisposto una informativa sul trattamento dei dati che è stata pubblicata sul sito istituzionale del comune		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Rischi di accesso non autorizzato ai dati	Perdita di dignità, violazione delle libertà per l'interessato	2	2	4	L'accesso alle banche dati viene fatto solo da soggetti autorizzati tramite utente protetto da password (Responsabile anticorruzione). Il comune ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati Il fornitore della piattaforma applicativa ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati come descritto nella documentazione tecnica fornita		
Rischi che i dati siano conservati per un periodo non necessario rispetto al trattamento.	Non rispetto nel principio di minimizzazione dei dati Riservatezza Integrità	1	2	2	Il tempo di conservazioni rispetta le finalità del trattamento inerenti la gestione della segnalazione e la necessità di gestire l'istruttoria		
Rischi che l'interessato possa avere difficoltà ad esercitare i suoi diritti (es. diritto alla cancellazione o modifica del dato) o che i suoi diritti vengano violati	Reclami degli interessati Sanzioni dell'autorità garante	1	2	2	I dati sono accessibili agli interessati attraverso procedure di accesso alla piattaforma Le policy di trattamento die dati sono descritte nell'informativa relativa al trattamento dei dati Il comune ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati Il fornitore della piattaforma applicativa ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati come descritto nella documentazione tecnica fornita		
Trattamento dei dati non conforme alla normativa di legge o alle linee guida dell'Autorità garante per la protezione dei dati.	Reclami degli interessati Sanzioni dell'autorità garante	2	2	4	I dati vengono raccolti per finalità legittime in base alle norme di legge in materia di whistleblowing. Verifica della corretta gestione delle procedure di trattamento dei dati e delle tecnologie utilizzate.		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Rischi fisici sede dell'ente							
Incendio	disponibilità Integrità	1	2	2	Impianti elettrici manutenuti in base alle norme di legge I locali dell'ente sono dotati di estintori		
Allagamento	disponibilità Integrità	1	2	2	L'edificio dell'ente è distante da corsi d'acqua e bacini idrici. Storicità dell'evento bassa		
Distruzione di strumentazione da parte di persone malintenzionate	disponibilità Integrità	1	2	2	Le misure di sicurezza dell'edificio sono adeguate, Storicamente non si sono mai verificati eventi di questo tipo Accesso ai locali in cui sono installati gli apparati del sistema informativo tramite porta chiudibile a chiave		
Attacchi Fisici, Furti, Atti vandalici	disponibilità Integrità	1	2	2	Le misure di sicurezza dell'edificio sono adeguate, Storicamente non si sono mai verificati eventi di questo tipo Accesso ai locali tramite porta chiudibile a chiave. Nell'edificio del comune è installato un impianto di allarme		
Fenomeni climatici - eventi calamitosi (Uragani, Nevicate)	disponibilità Integrità	1	2	2	Storicamente non si sono verificati eventi climatici dannosi		
Terremoti	disponibilità Integrità	1	2	2	Storicamente non si sono verificati eventi naturali dannosi quali terremoti Edificio antisismico / Rischio sismico basso		
Furto degli apparati	Disponibilità Riservatezza Integrità	2	2	4	I dispositivi sono installati in luoghi protetti e/o difficilmente accessibili; Nell'edificio del comune è installato un impianto di allarme		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Accesso non autorizzati a locali e/o in aree ad accesso ristretto	Riservatezza Integrità	2	1	2	I dispositivi di memorizzazione dei dati sono installati in locali ad accesso protetto;		
Sicurezza delle Rete Trasmissione Dati e della Rete Informatica dell'ente							
Rischi legati ad attacchi informatici	Disponibilità Riservatezza Integrità	2	2	4	L'ente ha adottato misure di sicurezza adeguate alla protezione dei dati (apparato di sicurezza perimetrale, software di protezione sugli apparati server e sulle postazioni di lavoro)		
Rischi legati all'accesso da parte di soggetti non autorizzati al trattamento dei dati	Disponibilità Riservatezza Integrità	1	2	2	L'accesso ai dati avviene tramite regole di autenticazione e profili diversi di accesso ai dati		
					Le società esterne che eseguono interventi di manutenzione ed assistenza sulla piattaforma applicativa sono state qualificate e nominate responsabili del trattamento dei dati ed il loro operato verificato dal personale della Polizia Locale		
Accesso non autorizzato ai locali per omessa sicurezza della struttura	Disponibilità Riservatezza Integrità	1	2	2	I locali nei quali sono installati gli apparati di informatici sono adeguatamente protetti (porta accesso sala server con serratura)		
Mancanza di energia elettrica o instabilità della stessa	Disponibilità	1	1	1	Evento raro con conseguenze accettabili Server alimentato con batterie di continuità		
Malfunzionamento per mancanza interventi di manutenzione che determinano anche delle vulnerabilità informatiche	Disponibilità Riservatezza Integrità	2	2	4	L'ente può contare su società specializzate nella manutenzione della piattaforma applicativa		
Intercettazione delle informazioni trasmesse sulla rete informatica	Riservatezza	1	2	2	La piattaforma applicativa utilizza protocolli sicuri di trasmissione dei dati		
Sicurezza della infrastruttura su cui è installata la piattaforma di whistleblowing							

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Rischi legati ad attacchi informatici	Disponibilità Riservatezza Integrità	2	2	4	Il fornitore della piattaforma applicativa ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati come descritto nella documentazione tecnica fornita. L'infrastruttura applicativa su cui è installata la piattaforma di whistleblowing è certificata ACN		
Rischi legati all'accesso da parte di soggetti non autorizzati al trattamento dei dati	Disponibilità Riservatezza Integrità	1	2	2	L'accesso ai dati avviene tramite regole di autenticazione e profili diversi di accesso ai dati		
					La società che gestisce la manutenzione e l'assistenza della piattaforma applicativa è stata nominata responsabile del trattamento dei dati		
Accesso non autorizzato ai locali per omessa sicurezza della struttura	Disponibilità Riservatezza Integrità	1	2	2	La piattaforma di whistleblowing è installata in un data center qualificato e dotato di idonee misure di sicurezza fisica		
Mancanza di energia elettrica o instabilità della stessa	Disponibilità	1	1	1	La piattaforma di whistleblowing è installata in un data center qualificato e dotato di idonee misure di sicurezza tecnologica		
Malfunzionamento per mancanza interventi di manutenzione che determinano anche delle vulnerabilità informatiche	Disponibilità Riservatezza Integrità	2	2	4	L'ente può contare su società specializzata nella manutenzione della piattaforma applicativa		
Intercettazione delle informazioni trasmesse sulla rete informatica	Riservatezza	1	2	2	La piattaforma applicativa utilizza protocolli sicuri di trasmissione dei dati La soluzione applicativa è installata su data center certificato AGID		
Rischi legati ai dati trattati dalla piattaforma di whistleblowing							
Modifica non autorizzata di dati	Riservatezza Integrità	1	2	2	I dati sono adeguatamente protetti per il livello di rischio legato alla modifica od alterazione degli stessi I dati sono salvato in modalità cifrata		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Comunicazione illecita o non corretta dei dati	Riservatezza	1	2	2	I dati trattati nel processo di whistleblowing non sono soggetti a comunicazione		
Mancata eliminazione dei dati al termine del trattamento	Riservatezza	2	2	4	I dati sono salvati in modalità cifrata I dati al termine dell'istruttoria possono essere cancellati dal segnalatore		
Trasferimento di dati all'estero	Riservatezza Mancato rispetto delle normative di legge	1	2	2	I dati relativi alla gestione del processo di whistleblowing non vengono trasferiti al di fuori dello spazio UE		
Danneggiamento delle banche	Disponibilità dei dati	1	2	2	Aggiornamento periodico della piattaforma applicativa Gestione delle copie dei server virtuali su cui è installata la piattaforma di whistleblowing		
Rischi legati all'applicazione software e agli apparati HW							
sottrazione/alterazione credenziali di autenticazione	Riservatezza Integrità	1	2	2	Le credenziali di accesso ai dati vengono periodicamente cambiate		
Policy di backup non adeguate problemi nelle procedure di gestione delle copie di sicurezza	Disponibilità	1	2	2	La piattaforma è installata su una struttura di server configurata in alta affidabilità. I server virtuali su cui è installata la piattaforma sono periodicamente copiati.		
Uso non autorizzato del software	Riservatezza	1	2	2	Le credenziali di accesso ai dati vengono periodicamente cambiate da parte del responsabile dell'anticorruzione da parte del responsabile dell'anticorruzione		
					I dati sono adeguatamente protetti per il livello di rischio legato al furto o all'accesso non autorizzato		
Malfunzionamento degli apparati o del sw di gestione dei dati	Riservatezza Integrità	2	2	4	Rischio di malfunzionamento degli apparati accettabile		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Mancato aggiornamento del software o errori di funzionamento	Riservatezza Integrità	1	2	2	Il software di gestione viene periodicamente aggiornato Attivato contratto di manutenzione della piattaforma applicativa di whistleblowing		
Rischi legati agli utenti							
Errori nel corretto trattamento dei dati da parte del titolare o da personale autorizzato	Disponibilità Riservatezza Integrità	1	2	2	Sensibilizzazione e formazione dei soggetti coinvolti nel trattamento; Istruzioni tecniche o formazione fornita al personale autorizzato al trattamento		
Non consapevolezza nelle procedure di gestione	Disponibilità Riservatezza Integrità	1	2	2	Il personale coinvolto nel trattamento è stato adeguatamente istruito; Il Comune si è avvalso di aziende o professionisti qualificati per l'attivazione della piattaforma di whistleblowing		
Non applicazione delle procedure di trattamento dei dati	Riservatezza Integrità	1	2	2	Sensibilizzazione e formazione dei soggetti coinvolti nel trattamento; Istruzioni tecniche o formazione fornita al personale autorizzato al trattamento		
Trattamento non corretto od illecito	Riservatezza Integrità	1	2	2	L'ente ha avviato procedure conformi alla normativa per una corretta gestione dei dati; I dati sono adeguatamente protetti sia con misure di carattere tecnologico che di protezione fisica		
Diffusione illecita delle immagini	Riservatezza	1	2	2	I dati relativi alla segnalazione di whistleblowing non sono soggetti a diffusione		
comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Disponibilità Riservatezza Integrità	1	3	3	I dati salvati dalla piattaforma di whistleblowing sono salvati in modalità cifrata		

11 Conclusione Finale

In seguito all’analisi effettuata, il trattamento non presenta particolari criticità in materia di protezione dei dati e rispetto dei diritti degli interessati per cui il Comune di Arcene non deve attuare azioni particolari nel processo di trattamento.

12 Allegati

Schede tecniche fornite da Whistleblowing Solutions I.S. S.r.l.

- WBIT - documentazione supporto DPIA
- WBIT - certificazione UNI CEI EN /IEC 27001:2017
- WBIT - conformità DNSH
- WBIT - modalità conservazione chiavi crittografiche
- WBIT - Informativa Privacy

WHISTLEBLOWINGIT

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

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

Documento aggiornato il 21 maggio 2025

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

SOMMARIO

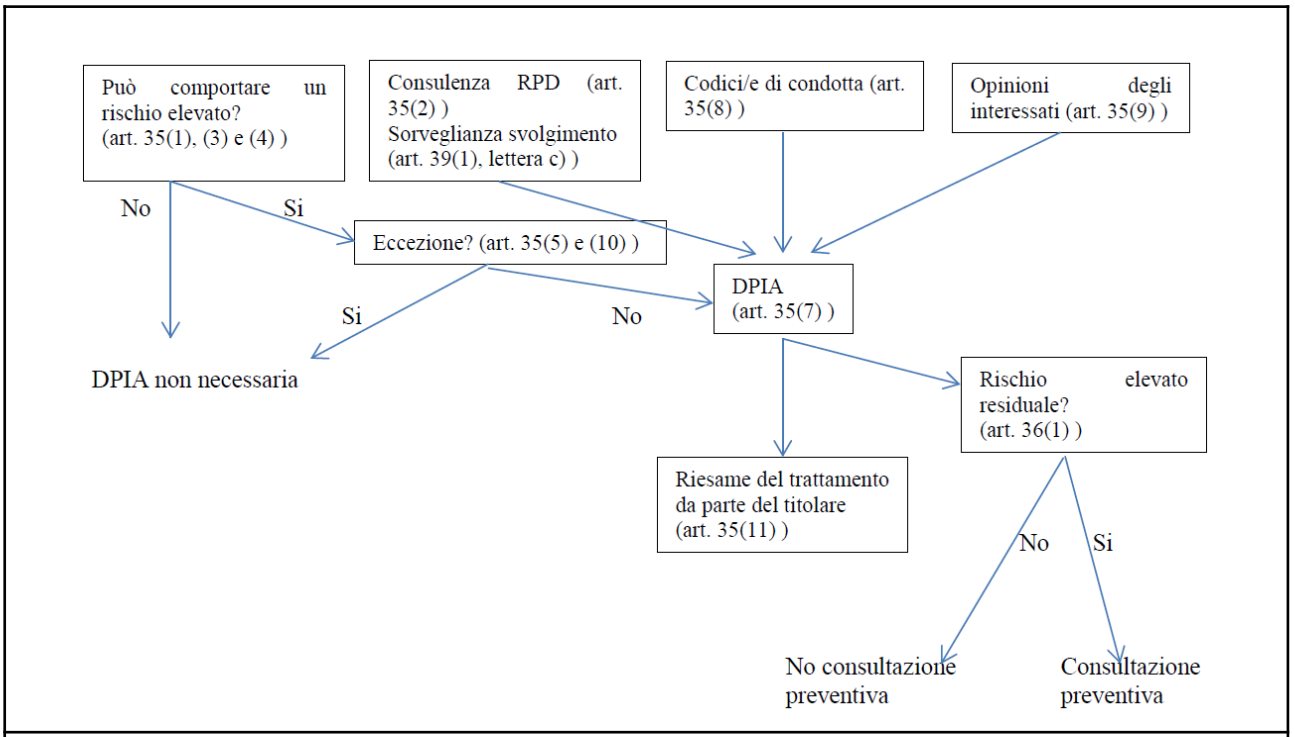
1. PREMESSA

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 **Gestore delle segnalazioni** > Soggetto autorizzato dal Titolare del Trattamento a trattare i dati relativi alle segnalazioni **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) **Transparency International Italia** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing
Standard applicabili	Il contesto normativo di riferimento richiede conformità a: • D.Lgs. n. 24/2023 o altra normativa nazionale in caso di entità giuridiche con sede in altro Paese. • DIRETTIVA (UE) 2019/1937 (WHISTLEBLOWING) • GENERAL DATA PROTECTION REGULATION - 2016/679 (GDPR) Il servizio erogato adotta misure progettate in aderenza allo standard internazionale ISO37002:2021 in materia di gestione dei processi di whistleblowing. Il Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato: • ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019 • ISO 9001:2015 • CSA STAR Level 1 • ACN

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.

	L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità di accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia. Al fine di consentire la possibilità di segnalazioni orali e al contempo tutelare l'anonimato e la confidenzialità, il sistema applica avanzate tecniche di "vocoding" (atte a evitare di raccogliere il timbro vocale) e "pitch shifting" (atte a variare il tono della voce in modo casuale) capaci di offrire elevate caratteristiche di anonimizzazione al passo con la ricerca nello specifico contesto d'uso. Tali tecniche permettono ai riceventi di ascoltare la registrazione senza essere in condizione di identificare la voce direttamente e rendendo altamente inefficaci tecniche moderne di de-anonimizzazione. Nonostante la registrazione venga protetta sotto questo profilo e venga mantenuta in forma alla pari di ogni allegato della segnalazione, per l'ascolto è indicato l'uso di cuffie per limitare l'esposizione del contenuto del messaggio.

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

Periodo di conservazione dei dati	Policy di data retention di default delle segnalazioni di 12 mesi, con cancellazione automatica sicura delle segnalazioni che raggiungono la data di scadenza. Il gestore può anticipare la scadenza delle segnalazioni fino a 3 mesi dalla data dell'operazione e può prorogare la scadenza delle segnalazioni per il tempo ritenuto congruo al trattamento dei dati. Anticipazioni e proroghe delle scadenze possono essere fatte dal gestore più volte. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.

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

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

5. MISURE DI SICUREZZA

CRITTOGRAFIA

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.

Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.

Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni.

Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento

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

Protocollo crittografico: https://docs.globaleaks.org/en/stable/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.

Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse.

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/stable/security/PenetrationTests.html

BACKUP

I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo dunque una RPO di 8 ore.

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

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.

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.

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

ISO/IEC 27001:2022

PER LE SEGUENTI ATTIVITÀ / *FOR THE FOLLOWING ACTIVITIES*

SETTORE CODE

IAF 33
LG 27017 27018

Progettazione, sviluppo, consulenza, installazione, fornitura, configurazione e manutenzione di software specifico di whistleblowing (GlobaLeaks), sia in modalità SaaS realizzata su infrastruttura di fornitori terzi che in modalità on-premise su infrastruttura dei clienti, compreso l'esercizio di tutte le attività preliminari, complementari, accessorie, commerciali e di assistenza.
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 31/01/2024.

Design, development, consultancy, installation, supply, configuration and maintenance of specific whistleblowing software (GlobaLeaks), both in SaaS mode created on third-party providers' infrastructure and on-premise mode on clients' infrastructure, including the execution of all preliminary, complementary, ancillary, commercial and assistance activities.
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 31/01/2024.

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*	*25/03/2024*
DATA SCADENZA *EXPIRY DATE*	*11/03/2026*
EMISSIONE CORRENTE *CURRENT ISSUE*	*25/03/2024*

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

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

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.

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

MODALITÀ DI CONSERVAZIONE DELLE CHIAVI CRITTOGRAFICHE

Documento aggiornato il 10 gennaio 2023

Opzione A – Conservazione delle Chiavi Crittografiche a cura del Fornitore

1. IDENTIFICAZIONE DEL BENE

1.1 Su espressa richiesta dell'ENTE, il FORNITORE provvede alla conservazione delle chiavi crittografiche necessarie a decrittare le informazioni presenti sulla Piattaforma ("Chiavi Crittografiche"). Tale misura di sicurezza è stata implementata per soddisfare i requisiti normativi e per proteggere adeguatamente i dati delle segnalazioni.

2. MODALITÀ DI RILASCIO E DI CONSEGNA DELLE CHIAVI

2.1 Il FORNITORE rilascerà le Chiavi Crittografiche dietro espressa richiesta scritta dell'ENTE.

2.2 Al fine di garantire la massima sicurezza dei processi di rilascio e consegna delle Chiavi Crittografiche, l'ENTE è tenuto ad indicare al FORNITORE un elenco di soggetti legittimati ad effettuare la relativa richiesta.

2.3 Il FORNITORE provvederà alla consegna delle Chiavi Crittografiche alle utenze indicate.

3. RESPONSABILITÀ DELLE PARTI

3.1 Il FORNITORE è tenuto a rendere le Chiavi Crittografiche prontamente disponibili all'ENTE, a condizione che la richiesta provenga dai soggetti autorizzati.

3.2 Il FORNITORE non si assume alcuna responsabilità circa la verifica dei presupposti che giustifichino il rilascio delle Chiavi Crittografiche, ritenendosi condizione sufficiente la richiesta proveniente dai soggetti legittimati.

3.3 La richiesta verrà evasa comunque durante il normale orario lavorativo, mentre potrebbero essere previsti dei costi aggiuntivi nel caso in cui la richiesta di messa a disposizione delle Chiavi Crittografiche dovesse avvenire al di fuori dell'orario lavorativo o durante giorni festivi.

3.4 Laddove le Chiavi Crittografiche vengano perse, distrutte o utilizzate in maniera non autorizzata per una causa imputabile all'ENTE, quest'ultimo manleverà e terrà indenne il FORNITORE da ogni responsabilità per danni, di qualsivoglia natura, causati all'ENTE, al FORNITORE e/o a terzi.

4. PERIODO DI ESCROW

4.1 Le Chiavi Crittografiche saranno conservate per l'intera durata del CONTRATTO tra l'ENTE e il FORNITORE. Successivamente alla sua conclusione, il FORNITORE procederà alla loro cancellazione sicura e non sarà possibile più accedere ai contenuti della piattaforma.

Opzione B – Conservazione delle Chiavi Crittografiche a cura dell'Ente

1. IDENTIFICAZIONE DEL BENE

1.1 L'ENTE è responsabile della conservazione delle chiavi crittografiche necessarie a decrittare le informazioni presenti sulla PIATTAFORMA ("Chiavi Crittografiche"). Tale misura di sicurezza è stata implementata per soddisfare i requisiti normativi e per assicurare che solo l'ENTE possa accedere ai dati delle segnalazioni.

2. MODALITÀ DI CUSTODIA

2.1 L'ENTE è responsabile della corretta e sicura conservazione delle Chiavi Crittografiche. In particolare, l'ENTE è tenuto a implementare tutte le misure tecniche ed organizzative necessarie ad assicurare la riservatezza, l'autenticità e l'integrità delle stesse.

3. RESPONSABILITÀ DELLE PARTI

3.1 L'ENTE è consapevole che la compromissione della riservatezza, dell'autenticità e dell'integrità delle Chiavi Crittografiche può comportare la compromissione della riservatezza, dell'autenticità e dell'integrità delle informazioni contenute sulla PIATTAFORMA e l'impossibilità di accedere alle stesse.

3.2. L'ENTE è l'unico soggetto responsabile per la conservazione delle Chiavi Crittografiche e manleva e tiene indenne il FORNITORE da ogni responsabilità per danni, di qualsivoglia natura, causati all'ENTE, al FORNITORE e/o a terzi dalla loro perdita, distruzione, e/o utilizzo non autorizzato.

INFORMATIVA PRIVACY

Documento aggiornato il 11 gennaio 2023

INFORMATIVA AI SENSI DELL'ART. 13 DEL REGOLAMENTO UE 2016/679

Il presente documento espone le modalità e le finalità del trattamento dei dati personali posto in essere da Whistleblowing Solutions Impresa Sociale S.r.l. (WBS), in qualità di titolare del trattamento (di seguito, anche il "Titolare" o il "Fornitore"), nonché ogni ulteriore informazione richiesta ai sensi di legge, ivi incluse le informazioni sui diritti dell'interessato e sul loro relativo esercizio.

Il Regolamento (UE) 2016/679 in materia di protezione dei dati personali (di seguito, il "Regolamento") stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati e protegge i diritti e le libertà fondamentali delle persone fisiche, con particolare riferimento al diritto alla protezione dei dati personali.

L'art. 4, n. 1 del Regolamento prevede che per "Dato Personale" debba intendersi qualsiasi informazione riguardante una persona fisica identificata o identificabile (di seguito, "Interessato").

Per "Trattamento" deve invece intendersi qualunque operazione o complesso di operazioni, effettuate 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 (art. 4, n. 2 del Regolamento).

Ai sensi degli artt. 12 e ss. del Regolamento, si prevede inoltre che l'Interessato debba essere messo a conoscenza delle opportune informazioni relative alle attività di Trattamento che sono svolte dal titolare del Trattamento e ai diritti degli Interessati.

TITOLARE DEL TRATTAMENTO
Titolare del Trattamento è Whistleblowing Solutions Impresa Sociale S.r.l. (WBS) con sede a Milano in Viale Abruzzi 13/A.

RESPONSABILE PROTEZIONE DEI DATI PERSONALI
Il titolare ha nominato il Responsabile per la Protezione dei Dati personali che può essere contattato scrivendo un'email a dpo@whistleblowingsolutions.it

FINALITÀ E BASE GIURIDICA
Il trattamento è finalizzato:

1. gestire, concludere e dare esecuzione al rapporto contrattuale concordato, nonché, degli eventuali dispositivi accessori richiesti, incluso ogni adempimento relativo ad obblighi fiscali e di contabilità;
2. all'assolvimento degli obblighi di legge.

MODALITÀ DEL TRATTAMENTO E CONSERVAZIONE
In conformità a quanto sancito dall'art. 5 del Regolamento, i Dati Personali oggetto di Trattamento sono:

1. trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato;
2. raccolti e registrati per finalità determinate, esplicite e legittime, e successivamente trattati in termini compatibili con tali finalità;

3. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. esatti e se necessario, aggiornati;
5. trattati in maniera da garantire un adeguato sicurezza;
6. conservati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

I Dati Personali saranno trattati dal Titolare con strumenti automatizzati e non automatizzati; la conservazione in forma elettronica dei Dati Personali avviene in server sicuri posti in aree ad accesso controllato e dotate di accessi ristretti.

Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

CONSERVAZIONE DEI DATI PERSONALI
I Dati Personali vengono conservati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti e sottoposti a Trattamento. Come principio generale, dunque, i Dati Personali verranno conservati per l'intero periodo di vigenza del rapporto con il Fornitore.

Resta inteso tuttavia che, venuto meno il rapporto contrattuale con il Fornitore e, con esso, le relative finalità del Trattamento, il Titolare sarà comunque obbligato e/o legittimato a conservare ulteriormente i Dati Personali, in tutto o in parte, per determinate finalità, come espressamente richiesto da specifiche previsioni di legge (ci si riferisce, per esempio, all'obbligo di tenuta delle scritture contabili per un periodo di 10 anni, previsto dall'art. 2220 del Codice Civile) o per far valere o difendere un diritto in sede giudiziaria (per esempio, in caso di possibili contestazioni rispetto alle attività svolte dal Fornitore).

COMUNICAZIONE DEI DATI PERSONALI
I Dati Personali saranno accessibili al Titolare agli incaricati del Trattamento e ai collaboratori esterni in relazione alle sole necessità di esecuzione del contratto e con precise nomine ai sensi ai sensi dell'art. 28 del Regolamento UE 2016/679.

Nello specifico sono nominati Sub-Responsabili del Trattamento:
- Transparency International Italia come partner di progetto;
- Seeweb S.r.l. come fornitore di infrastruttura.

DIFFUSIONE DEI DATI PERSONALI
I Dati Personali non sono soggetti a diffusione.

TRASFERIMENTO DEI DATI PERSONALI ALL'ESTERO
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.

COOKIE POLICY
Whistleblowing Solutions Impresa Sociale S.r.l. (WBS) è impegnata attivamente nella protezione dei propri clienti ed utenti e nella sensibilizzazione circa le tematiche di sicurezza informatica e privacy.
Come tale WBS sui propri siti utilizza solo cookies tecnici necessari per erogare i propri servizi ed in particolare solo cookies necessari all'autenticazione degli utenti e alla sicurezza dei propri siti e rinuncia all'utilizzo di qualsivoglia cookies di profilazione, di marketing e di terze parti.

DIRITTI DELL'INTERESSATO
In qualsiasi momento l'Interessato potrà accedere ai Dati Personali al fine di correggerli, eliminarli e, in generale, esercitare tutti i diritti che gli sono espressamente riconosciuti ai sensi della normativa applicabile in materia di protezione dei Dati Personali, e in dettaglio: il diritto di ottenere la conferma dell'esistenza o meno dei Dati Personali e la loro comunicazione in forma intelligibile, di conoscerne

l'origine, le finalità e le modalità del Trattamento; il diritto di ottenere l'indicazione degli estremi identificativi del Titolare, dei responsabili del trattamento e dei soggetti o delle categorie di soggetti ai quali i Dati Personali possono essere comunicati; il diritto di verificare l'esattezza dei Dati Personali o chiederne l'integrazione o l'aggiornamento oppure la rettificazione; il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei Dati Personali trattati in violazione alla legge, nonché la loro limitazione ai sensi di legge e di opporsi in ogni caso, in tutto o in parte, per motivi legittimi al loro Trattamento; il diritto alla portabilità dei propri Dati Personali, nonché il diritto di proporre un reclamo, una segnalazione o un ricorso al Garante per la protezione dei dati personali, ove ne ricorrano i presupposti. La normativa applicabile riconosce, inoltre, il diritto di revocare il proprio consenso al Trattamento dei Dati Personali in qualsiasi momento, senza che ciò pregiudichi, tuttavia, la liceità del Trattamento posto in essere dal Titolare sulla base del consenso prestato prima della revoca.

ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Per esercitare i propri diritti l'Interessato può rivolgersi in qualsiasi momento al Titolare del Trattamento scrivendo un'email a gdpr@whistleblowing.it.