ARNAS G.Brotzu
Azienda di Rilievo Nazionale
ed Alta Specializzazione

WHISTLEBLOWING

DECRETO LEGISLATIVO n. 24 del 10 marzo 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".

D.P.I.A. "DATA PROTECTION IMPACT ASSESSMENT"
VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI
(art.35 Regolamento UE/2016/679 "GDPR")

INDICE

Premessa

La DPIA, acronimo di *Data Protection Impact Assessment*, è una valutazione preliminare, eseguita dal Titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati. In linea con l'approccio basato sul rischio adottato dal Regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche", ai sensi dell'art. 35 del Regolamento UE 2016/679 (di seguito anche "GDPR").

Il GDPR introduce dunque una valutazione di stampo preliminare, che consente al Titolare del trattamento di prendere visione del rischio prima ancora di procedere al trattamento e di attivarsi perché tale rischio possa essere, se non annullato, quantomeno fortemente ridotto.

I principi fondamentali della DPIA risultano pertanto:

- i diritti e le libertà fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR;
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio.

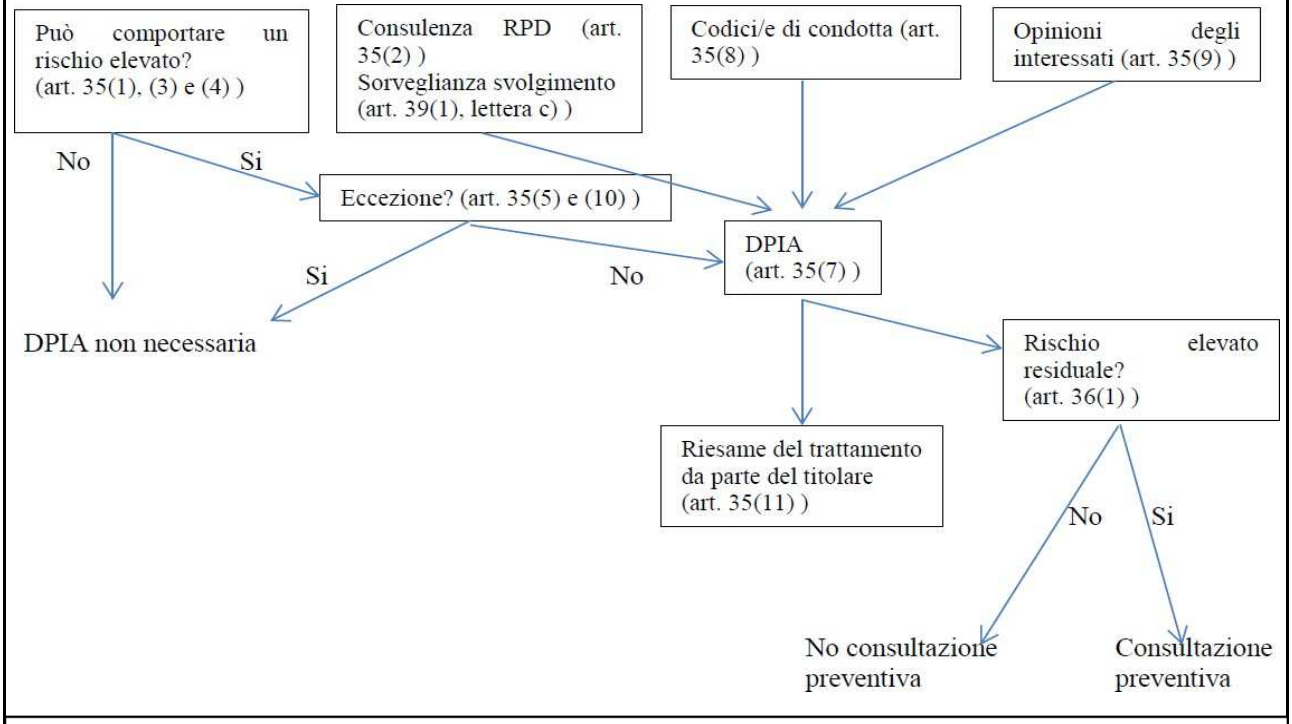
Una DPIA poggia su due pilastri:

1. i principi e i diritti fondamentali, i quali sono "non negoziabili", stabiliti dalla legge e che devono essere rispettati e non possono essere soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi;
2. la gestione dei rischi per la privacy dei soggetti interessati, che determina i controlli tecnici e organizzativi opportuni a tutela dei dati personali.

Normativa di riferimento

Ai fini della redazione del presente atto si fa riferimento specificatamente ai seguenti atti normativi:

- 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 (regolamento generale sulla protezione dei dati).
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato e integrato dal Decreto Legislativo 10 agosto 2018 n.101.
- Legge 30 novembre 2017, n. 179 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato."
- Legge 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e della illegalità nella pubblica amministrazione."
- Decreto Legislativo 10 marzo 2023, n. 24 "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."



Principi fondanti il processo di DPIA

DESCRIZIONE DELLA PIATTAFORMA DI WHISTLEBLOWING

Whistleblowing Solutions, in qualità di Responsabile del trattamento, 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 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.

DESCRIZIONE E ANALISI DEL CONTESTO

Dati del DPO: Avv. Giovanni Battista Gallus
Mail: dpo@aob.it

Parere del DPO:

I. Premessa

La presente valutazione d'impatto sulla protezione dei dati (DPIA) si basa sull'analisi condotta del sistema di whistleblowing adottato dall'ARNAS G. Brotzu, conformemente al Decreto Legislativo 10 marzo 2023 n. 24, che recepisce la Direttiva (UE) 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione. La DPIA valuta i rischi associati al trattamento dei dati personali nel contesto delle segnalazioni di illeciti e verifica le misure adottate per mitigare tali rischi.

II. Analisi del Trattamento

Il sistema di whistleblowing consente ai segnalanti di inoltrare segnalazioni di illeciti in modo confidenziale e, ove possibile, anonimo. Il trattamento dei dati personali riguarda i dati del segnalante e di altri soggetti potenzialmente coinvolti, in linea con le finalità di prevenzione della corruzione e tutela dell'integrità dell'ente.

III. Responsabilità:

- ARNAS G. Brotzu: Titolare del trattamento.
- Whistleblowing Solutions: Responsabile del trattamento.
- Sub-responsabili: Seeweb (gestione infrastruttura) e Transparency International Italia (supporto operativo).

IV. Valutazione delle Misure di Sicurezza

La DPIA evidenzia l'adozione di misure di sicurezza adeguate e proporzionate per garantire la protezione dei dati personali trattati. Tra queste misure, risultano centrali:

- **Crittografia**: I dati sono protetti da crittografia avanzata sia in transito che a riposo, riducendo significativamente i rischi di accesso non autorizzato.
- **Controllo degli accessi**: Implementazione di policy di accesso con autenticazione a due fattori e controllo degli accessi logici, limitando l'accesso ai soli soggetti autorizzati.
- **Tracciabilità**: Sistema di audit log che garantisce la registrazione delle attività senza compromettere la privacy e l'anonimato dei segnalanti.
- **Backup e Gestione delle Vulnerabilità**: Backup giornaliero con politiche di retention e controlli periodici per garantire la resilienza del sistema.

V. Rischi Identificati e Valutazione

La DPIA ha identificato i seguenti principali rischi:

- **Accesso illegittimo ai dati**: Rischio mitigato tramite l'uso di crittografia robusta e controlli di accesso.
- **Modifiche indesiderate dei dati**: Rischio ridotto grazie a misure di tracciabilità e sicurezza logica.
- **Perdita di dati**: Rischio considerato limitato grazie a politiche di backup e disaster recovery.

Tutti i rischi risultano essere valutati come "accettabili" grazie alle misure implementate.

VI. Conclusioni e Raccomandazioni

Il sistema di whistleblowing dell'ARNAS G. Brotzu, basato sulla piattaforma GlobaLeaks, rispetta i requisiti imposti dal GDPR e dalla normativa nazionale in materia di whistleblowing. Le misure tecniche e organizzative implementate sono adeguate per garantire un elevato livello di protezione dei dati personali, minimizzando i rischi per i diritti e le libertà fondamentali degli interessati.

Raccomandazioni del DPO:

- Continuare a monitorare l'efficacia delle misure di sicurezza attraverso audit periodici.
- Rafforzare le procedure per la gestione degli incidenti di sicurezza, con particolare attenzione alla formazione continua del personale.
- Prevedere una revisione periodica delle valutazioni del rischio in funzione dell'evoluzione delle minacce e delle tecnologie.

In conclusione, la valutazione d'impatto conferma la conformità del sistema con le normative applicabili, con un adeguato bilanciamento tra la protezione dei dati personali e l'obbligo legale di gestire le segnalazioni di illeciti.

Per ulteriori approfondimenti o modifiche delle misure di sicurezza, si raccomanda un costante aggiornamento delle prassi operative alla luce delle evoluzioni normative e tecnologiche.

Cagliari, li 04.08.2024

Avv. Giovanni Battista Gallus
Responsabile della Protezione dei Dati (DPO)

Richiesta Del Parere Degli Interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
Il fondamento giuridico del trattamento dei dati risiede nell'assolvimento di funzioni ed obblighi di legge.

1. CONTESTO

1.1 Panoramica del trattamento

Responsabilità connesse al trattamento:	**ARNAS G. Brotzu**> 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.

Quale è il trattamento in considerazione?

L'istituto del whistleblowing è uno strumento che si prefigge di regolamentare e facilitare la segnalazione di illeciti di cui il soggetto segnalante, il cosiddetto "whistleblower", sia venuto a conoscenza nell'ambito del proprio contesto lavorativo, anche mediante la previsione di significative forme di tutela nei confronti dello stesso segnalante e degli altri soggetti coinvolti.
In Italia, il whistleblowing è regolato dal nuovo decreto entrato in vigore dal 15 luglio 2023 "D.Lgs. 10 marzo 2023, n. 24" e dalle "Linee guida dell'Autorità Nazionale Anticorruzione".

L'ARNAS G. Brotzu mette a disposizione dei dipendenti e collaboratori di imprese fornitrici di beni e servizi, un nuovo strumento per contrastare la corruzione. Si tratta di una piattaforma informatica https://arnasgbrotzu.whistleblowing.it/ che permette di inviare segnalazioni di illeciti di cui si è venuti a conoscenza in maniera sicura e confidenziale.

Il trattamento dei dati riguarda pertanto i dati di cui agli artt. 6-9-10 del Regolamento UE 2016/679 riconducibili al segnalante ma esteso anche ai seguenti soggetti:

- al facilitatore (persona fisica che assiste il segnalante nel processo di segnalazione e operante all'interno del medesimo contesto lavorativo);
- alle persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente.

Quali sono le responsabilità connesse al trattamento?

L'ARNAS G. Brotzu ha affidato all'esterno la gestione della piattaforma informatica per la gestione delle segnalazioni di illeciti, in modalità cloud, attraverso la quale il segnalante ha la possibilità di inviare la segnalazione.

Il fornitore è stato designato Responsabile del trattamento dei dati, ai sensi dell'art. 28 del Regolamento UE 2016/679.

La riservatezza è garantita attraverso idoneo sistema di crittografia.

Valutazione: Accettabile

Standard applicabili:	**Conformità normativa:** ● 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.

Ci sono standard applicabili al trattamento?

L'ANAC ha pubblicato, con delibera n. 311 del 12 luglio 2023, le nuove "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne."
Tali linee guida forniscono indicazioni e princìpi di cui gli enti pubblici e privati possono tener conto per i propri canali e modelli organizzativi interni, su cui ANAC si riserva di adottare successivi atti di indirizzo. Si fa presente che, laddove possibile, i contenuti della nuova disciplina sono stati messi a confronto con quella previgente al fine di consentire agli interessati di poter valutare le principali innovazioni introdotte a seguito della Direttiva UE 2019/1937.

Valutazione: Accettabile

1.2 Dati, processi e risorse di supporto

Dati e operazioni di trattamento:	**Quali sono i dati trattati?** 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.

Attraverso il portale whistleblowing possono essere trattati dati personali e particolari di cui agli artt. 6-9-10 del Regolamento UE 2016/679, considerando che il segnalante ha facoltà di riportare i fatti accaduti integrando informazioni molto riservate riconducibili a terzi.

Valutazione: Accettabile

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.

Quale è il ciclo di vita del trattamento dei dati? (descrizione funzionale)
Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonchè dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33. Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del decreto legislativo n. 24 del 2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del Regolamento UE 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

Valutazione: Accettabile

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).

Quali sono le risorse di supporto ai dati?

I dati sono gestiti mediante un' apposita piattaforma attivata dall'ARNAS G. Brotzu basata sul riuso del software GlobalLeaks e personalizzata dal Settore Servizi Informatici e Telematici dell'ARNAS G. Brotzu, per l'acquisizione e la gestione (nel rispetto delle garanzie di riservatezza previste dalla normativa vigente) delle segnalazioni di illeciti da parte dei dipendenti dell' Azienda, dialogare con i segnalanti anche in modo anonimo così come previsto dal Decreto Legislativo 24 del 2023 e previsto dalle Linee Guida ANAC.
GlobalLeaks è un software open-source creato per permettere l'avvio di iniziative di whistleblowing sicuro ed anonimo rilasciato sotto licenza AGPL (Affero General Public License).

Valutazione: Accettabile

2. PRINCIPI FONDAMENTALI

2.1 Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati personali sono trattati nel rispetto dei principi di cui all'art. 5 del Regolamento UE 2016/679. fornendo adeguata informativa ai segnalanti attraverso il sito internet istituzionale e prima dell'accesso alla piattaforma web, ai sensi degli artt. 13-14 del Regolamento UE 2016/679.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

I dati personali sono trattati dal Responsabile della prevenzione della corruzione e della trasparenza dell'ARNAS G. Brotzu per obbligo di legge e 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 pubblico e dell'integrità dell'ARNAS G. Brotzu, ai sensi del D.Lgs 24/2023.

Valutazione: Accettabile

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.

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

Il trattamento dei dati personali verrà effettuato esclusivamente dal Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) dell'ARNAS G. Brotzu, con l'utilizzo di procedure anche informatizzate, dotate di strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e del contenuto delle segnalazioni e della relativa documentazione, adottando misure tecniche e organizzative adeguate a proteggerli da accessi non autorizzati o illeciti, dalla distruzione, dalla perdita d'integrità e riservatezza, anche accidentali.

I dati verranno conservati per 5 anni e comunque per tutta la durata dell'eventuale procedimento disciplinare, penale o dinanzi la Corte dei Conti. I dati personali non saranno comunicati ad altri soggetti, ad esclusione dei casi sopra indicati, così come non saranno oggetto di diffusione.

Valutazione: Accettabile

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.

I dati sono esatti e aggiornati?

Al fine della verifica della correttezza e dell'aggiornamento dei dati, si stabilisce la prima verifica entro 6 (sei) mesi dalla redazione del presente documento.

Valutazione: Accettabile

Periodo di conservazione dei dati	**Quale è il periodo di conservazione dei dati?** Policy di data retention di default delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma. **Valutazione: Accettabile**

2.2 Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati che accedono al Portale whistleblowing sono invitati a prendere visione dell'informativa sul trattamento dei dati personali pubblicata sul sito istituzionale dell'ARNAS G. Brotzu, nell'apposita sezione Privacy.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

I dati personali del segnalante sono raccolti e trattati dal Responsabile della Prevenzione della Corruzione e della Trasparenza per obbligo di legge e dagli autorizzati dell'Ufficio Anticorruzione, con particolare riferimento al compito di accertare eventuali illeciti denunciati nell'interesse pubblico e dell'integrità aziendale, ai sensi del D.Lgs. n. 24 del 10 marzo 2023, recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

In alcuni casi, inoltre, in base a quanto previsto dai seguenti articoli del D.Lgs. 10 marzo 2023 n. 24, potrebbe essere richiesto il consenso espresso, specifico e libero dell'interessato (art. 6, par. 1, lett. a GDPR):

- Art. 12 comma 2: la rivelazione dell'identità della persona segnalante a persone diverse da quelle competenti a ricevere o dare seguito alle segnalazioni può avvenire solo previo consenso espresso della stessa persona segnalante;
- Art. 12 comma 5: qualora, nell'ambito del procedimento disciplinare, la conoscenza dell'identità del segnalante fosse indispensabile per la difesa dell'incolpato, verrà domandato al segnalante se intende rilasciare il consenso ai fini della rivelazione della propria identità.

Il trattamento dei dati è necessario per dare attuazione agli obblighi di legge e ai compiti d'interesse pubblico previsti dalla disciplina di settore la cui osservanza è condizione di liceità del trattamento.

Valutazione: Accettabile

Come fanno gli interessati ad esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati del trattamento possono esercitare i diritti di cui sopra, nei limiti di cui all'art. 2-undecies del codice Privacy, inviando una mail al DPO all'indirizzo: dpo@aob.it.

Valutazione: Accettabile

Come fanno gli interessati ad esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati del trattamento possono esercitare i diritti di cui sopra, nei limiti di cui all'art. 2-undecies del codice Privacy, inviando una mail al DPO all'indirizzo: dpo@aob.it.

Valutazione: Accettabile

Come fanno gli interessati ad esercitare i loro diritti di limitazione e di opposizione?

Gli interessati del trattamento possono esercitare i diritti di cui sopra, nei limiti di cui all'art. 2-undecies del codice Privacy, inviando una mail al DPO all'indirizzo: dpo@aob.it.

Valutazione: Accettabile

Definizione degli obblighi dei responsabili del trattamento e formalizzazione dei contratti	**Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?** 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. **Valutazione: Accettabile**
Protezione in caso di trasferimento di dati al di fuori dell'Unione europea:	**In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?** 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. **Valutazione: Accettabile**

3. VALUTAZIONE DEL SISTEMA

3.1. Misure esistenti o pianificate

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 **Valutazione: Accettabile**

Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati dal Responsabile per la prevenzione della corruzione e della trasparenza (RPCT) dell'ARNAS G. Brotzu che verifica che siano disposti in specifici raccoglitori in modo tale che non vadano dispersi e che non siano visibili a terzi non autorizzati, gli uffici devono essere chiusi e l'accesso consentito soltanto agli addetti o i soggetti autorizzati.

Valutazione: Accettabile

Specifiche misure di sicurezza

Il Titolare del trattamento e il responsabile per la prevenzione della corruzione e della trasparenza, previa valutazione dei rischi, mettono in atto misure volte a:

- vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);
- impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);
- impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);
- impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);
- garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);
- garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);
- garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);
- impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);
- garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);
- garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Valutazione : Accettabile

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. **Valutazione: Accettabile**
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. **Valutazione: Accettabile**
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. **Valutazione: Accettabile**
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 **Valutazione: Accettabile**
Backup	I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery. **Valutazione: Accettabile**
Manutenzione	È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti. Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti. **Valutazione: Accettabile**

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. **Valutazione: Accettabile**
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. **Valutazione: Accettabile**
Gestione degli incidenti di sicurezza e delle violazioni dei dati personali	Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali. **Valutazione: Accettabile**
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. **Valutazione: Accettabile**

4. RISCHI

4.1 Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Mobbing, discriminazione, isolamento, perdita dignità, perdita lavoro. Qualora fosse realizzato un accesso abusivo al sistema da soggetti attrezzati e travisati e fosse possibile asportare la memoria di massa senza il pronto intervento dei sistemi di sicurezza, i dati sarebbero crittografati. Quindi si tratterebbe di un impatto limitato.

Quali sono le principali minacce che potrebbero concretizzare il rischio?
Comunicazione dati segnalante, diffusione dati segnalante.

Quali sono le fonti di rischio?
Fonti umane interne, fonti umane esterne, cause naturali.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Specifiche misure di sicurezza (crittografia, lotta contro il malware, controllo degli accessi logici).

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata, poiché il sistema di crittografia e il posizionamento del computer di accesso in un locale sicuro e presidiato, rendono molto limitato il rischio di accesso abusivo ai dati e limitato il rischio di distruzione degli stessi.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Limitata, sulla base delle misure pianificate.

Valutazione: Accettabile

4.2 Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio dovesse concretizzarsi?
Mobbing, discriminazione, isolamento, perdita dignità, perdita lavoro. Qualora fosse realizzato un accesso abusivo al sistema da soggetti attrezzati e travisati e fosse possibile asportare la memoria di massa senza il pronto intervento dei sistemi di sicurezza, i dati sarebbero crittografati. Si tratterebbe pertanto di un impatto limitato.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?
Malfunzionamento software, alternazione volontaria di dati, virus, alterazione accidentale di dati. Danno fisico hardware, vulnerabilità software, vulnerabilità database.

Quali sono le fonti di rischio?
Fonti umane interne, fonti umane esterne, cause naturali.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Specifiche misure di sicurezza (crittografia, backup, tracciabilità, vulnerabilità, lotta contro il malware, gestire gli incidenti di sicurezza e le violazioni dei dati personali, anonimizzazione, sicurezza dei siti web, controllo degli accessi logici, manutenzione). Messa in sicurezza dei documenti cartacei.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Limitata, il sistema di crittografia e il controllo logico degli accessi rende pressoché impossibile l'accesso ai dati ai fini della modifica se non ai soggetti autorizzati e quindi formati e competenti.

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

Limitata. La probabilità di accadimento del rischio di modifiche non desiderate ai dati è stimata come limitata in considerazione delle misure di sicurezza implementate.

Valutazione: Accettabile

4.3 Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Perdita delle informazioni, perdita del controllo sui dati.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?
Furto, vandalismo, virus, danno fisico hardware, cancellazione volontaria, cancellazione accidentale.

Quali sono le fonti di rischio?
Fonti umane interne, fonti umane esterne, cause naturali.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Specifiche misure di sicurezza (crittografia, backup, tracciabilità, vulnerabilità, lotta contro il malware, gestire gli incidenti di sicurezza e le violazioni dei dati personali, anonimizzazione, sicurezza dei siti web, controllo degli accessi logici, manutenzione). Messa in sicurezza dei documenti cartacei.

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

Limitata. La gravità del rischio è stimata come limitata in considerazione delle misure di sicurezza applicate (backup giornaliero con policy di data retention di 7 giorni).

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

Limitata. La probabilità di accadimento del rischio di perdita dei dati è bassa in considerazione delle misure di sicurezza applicate

Valutazione: Accettabile

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 di altre misure al passo con la ricerca e la tecnica in ambito di sicurezza informatica reperibile alle seguenti pagine web:

a. THREAT MODEL
b. APPLICATION SECURITY