Oggetto: valutazione di impatto sulla protezione dei dati personali (c.d. "DPIA") relativa al trattamento di dati personali realizzato per l'attuazione della normativa in materia di c.d. "Whistleblowing" di cui al d.lgs. 24/2023.

Premessa

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), la DPIA corrisponde alla valutazione d'impatto del trattamento del dato sulla protezione dei dati personali, qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ciò considerata la natura, il contesto e le finalità del trattamento.
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.
La Metodologia di analisi dei rischi adottata nella conduzione delle attività di Data Privacy Impact Assessment è la metodologia di analisi CNIL del Garante Francese (o altra metodologia definita dal Titolare del trattamento).

1. CONTESTO

a) Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi del D.lgs. n. 24/2023.

La gestione delle segnalazioni viene effettuata attraverso una piattaforma on-line scelta dalla dall'Ordine della Professione Ostetrica della Provincia di Ravenna (di seguito "**Ordine**").

La piattaforma svolge funzioni di raccolta e gestione delle segnalazioni di illeciti per contrastare fenomeni corruttivi, sia nelle imprese private sia nelle pubbliche amministrazioni.

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.

Di seguito si riportano le principali caratteristiche della piattaforma:

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.

Piazza Bernini n.2 - 48124 Ravenna; Tel. 0544/402543 - PEC: ravennaost@pec.aruba.it - C.F. 80008190391

	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. 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

Piazza Bernini n.2 - 48124 Ravenna; Tel. 0544/402543 - PEC: ravennaost@pec.aruba.it - C.F. 80008190391

	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.

b) Responsabilità connesse al trattamento

Ruolo	**Nominativo**
Titolare del trattamento	Ordine della Professione Ostetriche della Provincia di Ravenna.
Responsabile del trattamento	Whistleblowing Solutions (per la fornitura e la gestione del sistema whistleblowing)
Sub Responsabile	Seeweb (per la gestione dell'infrastruttura Iaas) Transparency International Italia (per la collaborazione nella gestione del sistema whistleblowing)
Autorizzati al trattamento	RPCT

c) Standard applicabili

Al trattamento in materia di segnalazioni e normativa whistleblowing si applicano le seguenti normative e standard:

- Regolamento UE n. 2016/679 (c.d. GDPR)
- D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018
- Direttiva UE 1937/2019
- D.lgs. n. 24/2023
- Linee Guida ANAC
- ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks"
- ISO27017 controlli di sicurezza sulle informazioni per i servizi Cloud
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud
- Qualifica AGID del fornitore della piattaforma
- Certificazione CSA Star del fornitore della piattaforma

d) Dati, processi e risorse di supporto

Di seguito si riportano le tipologie di dati personali che sono oggetto di trattamento a seguito di una segnalazione fatta ai sensi del D.lgs. n. 24/2023:

Categoria di dato personale	**Categoria di interessato**
Dati personali comuni e di contatto	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Componenti degli organi politici che effettuano una segnalazione o che ne sono oggetto

Piazza Bernini n.2 - 48124 Ravenna; Tel. 0544/402543 - PEC: ravennaost@pec.aruba.it - C.F. 80008190391

	Fornitori che effettuano una segnalazione o vengono segnalati
Dati personali particolari (es. dati relativi alla salute, dati relativi all'appartenenza sindacale)	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Componenti degli organi politici che effettuano una segnalazione o che ne sono oggetto Fornitori che effettuano una segnalazione o vengono segnalati
Dati giudiziari (es. condanne penali)	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Componenti degli organi politici che effettuano una segnalazione o che ne sono oggetto Fornitori che effettuano una segnalazione o vengono segnalati

e) Ciclo di vita del trattamento 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 (RPCT);
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.

f) Risorse a supporto dell'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)

2. PRINCIPI FONDAMENTALI

a) Proporzionalità e necessità

Gli scopi dei trattamenti sono specifici, espliciti e legittimi?

Il trattamento è finalizzato esclusivamente alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing.

Quali sono le basi giuridiche che rendono lecito il trattamento?

Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui è tenuto il titolare (Art. 6.1. lett. c) GDPR).

Piazza Bernini n.2 - 48124 Ravenna; Tel. 0544/402543 - PEC: ravennaost@pec.aruba.it - C.F. 80008190391

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

Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, E-mail 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 l'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.

In ogni caso, i dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D.lgs. n. 24/2023.

A seconda di quanto contenuto nella singola segnalazione ricevuta, e sulla base delle informazioni fornite, l'Ordine potrà trattare eventualmente categorie particolari di dati ex art. 9 GDPR.

I dati sono esatti e aggiornati?

Il trattamento dei dati personali relativi alle segnalazioni sono costantemente aggiornati in quanto i soggetti incaricati di ricevere e gestire le segnalazioni ne verificano preliminarmente la corrispondenza a verità.

Qual è il periodo di conservazione dei dati?

La Policy di data retention di default della piattaforma prevede in periodo di conservazione dei dati 12 mesi, prorogabili al doppio su singole segnalazioni, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere dal soggetto gestore delle segnalazioni più volte.

In ogni caso, le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 14/2023.

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

Come sono definiti gli obblighi dei responsabili del trattamento?

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.

I dati personali sono trasferiti extra UE?

Piazza Bernini n.2 - 48124 Ravenna; Tel. 0544/402543 - PEC: ravennaost@pec.aruba.it - C.F. 80008190391

I dati personali sono trattati principalmente in Italia ed esclusivamente nei paesi dell'Unione Europea.

Non vi è alcun trasferimento di dati personali verso l'estero in paesi extra UE.

b) Misure a tutela dei diritti e delle libertà degli interessati

Come sono informati del trattamento gli interessati?

Mediante l'informativa sul trattamento pubblicata sul sito web, nella sezione dedicata al "Whistleblowing".

Ove applicabile: come si ottiene il consenso degli interessati?

Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita in linea generale di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (art. 6.1 lett. c) del GDPR).

Come fanno gli interessati a esercitare i loro diritti previsti dagli artt. 15 ss. GDPR?

Cfr. documento di lavoro, normativa in esame e Linee guida ANAC in materia per i limiti a tali diritti. Al di fuori di tali limiti, le modalità di esercizio dei diritti sono descritte nell'informativa sul trattamento. Se è già stato adottato il protocollo in materia di esercizio dei diritti degli interessati, l'esercizio dei diritti può avvenire mediante apposito modulo pubblicato sul sito web dell'ente.

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

Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del trattamento ai sensi dell'art. 28 GDPR, attraverso contratti o altri atti giuridici.

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

Non è previsto un trasferimento di dati personali fuori dall'Unione Europea.

3. RISCHI

Per la valutazione dei rischi, le Linee guida ANAC evidenziano che è necessario "Effettuare il trattamento in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). Nel contesto in esame, caratterizzato da elevati rischi per i diritti e le libertà degli interessati, il ricorso a strumenti di crittografia nell'ambito dei canali interni di segnalazione, è di regola da ritenersi una misura adeguata a dare attuazione, fin dalla progettazione e per impostazione predefinita, al predetto principio di integrità e riservatezza. Le misure di sicurezza adottate devono, comunque, essere periodicamente riesaminate e aggiornate".

A fronte di quanto sopra e della rilevanza che hanno riservatezza, integrità e disponibilità dei dati nel contesto in esame, la valutazione dei rischi potenziali può essere esemplificata ritenendo:

- elevato il rischio di impatto per la perdita di riservatezza dell'identità del segnalante, salvo i casi di divulgazione pubblica delle segnalazioni o le ipotesi in cui l'identità può essere comunicata ai soggetti indicati nell'art. 12 del d.lgs. 24/2023;

Piazza Bernini n.2 - 48124 Ravenna; Tel. 0544/402543 - PEC: ravennaost@pec.aruba.it - C.F. 80008190391

- medio il rischio di impatto per la perdita di disponibilità, considerato che il soggetto potrebbe nuovamente procedere alla segnalazione (N.B.: le segnalazioni anonime, sono gestite come ordinarie, pertanto non sono considerate per la valutazione del rischio) e comunque essere coinvolto nel seguito che ne deriva, nonché rivolgersi all'ANAC o all'autorità giudiziaria in caso la segnalazione non vada in porto (in tal senso, la perdita di disponibilità appare costituire un rischio più per l'Ente che per i diritti e le libertà degli interessati).

a) Misure di sicurezza esistenti

Crittografia	L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington. Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto. Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html
Controllo degli accessi logici	L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.
Tracciabilità	L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.
Archiviazione	L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.
Gestione delle vulnerabilità tecniche	L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio

Piazza Bernini n.2 - 48124 Ravenna; Tel. 0544/402543 - PEC: ravennaost@pec.aruba.it - C.F. 80008190391

	respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente. Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html
Backup	I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.
Manutenzione	E' prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema e 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 e 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 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24. I datacenter del fornitore IaaS sono certificati ISO27001.
Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Gli incidenti di sicurezza e le violazioni dei dati personali vengono gestiti secondo la "Procedura Data Breach" adottata dal Titolare in conformità a quanto prescritto dagli artt. 33-34 del GDPR.
Vigilanza sulla protezione dei dati	Vigilanza svolta da DPO/funzioni incaricate dal titolare del trattamento.

b) Panoramica dei rischi

Secondo le Linee guida ANAC le misure indicate risultano adeguate alla mitigazione dei rischi individuati , che pertanto non risultano elevati.

4. PARERE DELLE PARTI INTERESSATE

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge.

5. PARERE DPO

Piazza Bernini n.2 - 48124 Ravenna; Tel. 0544/402543 - PEC: ravennaost@pec.aruba.it - C.F. 80008190391

Il DPO esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo.

6. CONCLUSIONI

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emerge che, con l'implementazione delle misure tecnico/organizzative adottate, il valore di rischio residuo rientra nei parametri accettabili, valore ritenuto accettabile dall'organizzazione in relazione dai parametri oggettivi considerati.

Si ritiene pertanto che il trattamento in oggetto presenti un grado di rischio sui diritti e libertà dell'interessato rientrante nei parametri accettabili e di conseguenza non è richiesta una consultazione preventiva all'Autorità Garante.

7. VALIDAZIONE

La sottoscritta Gasperoni Oriana in qualità di Presidente e l.r.p.t. dell'ente per la sua validazione.

Ravenna, 14/04/2026

ORDINE DELLA PROFESSIONE DI OSTETRICA di RAVENNA

La Presidente
Gasperoni Oriana

Piazza Bernini n.2 - 48124 Ravenna; Tel. 0544/402543 - PEC: ravennaost@pec.aruba.it - C.F. 80008190391