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 "WHISTLEBLOWING" DI CUI AL D.LGS. 24/2023

Premessa

L'Ordine Dei Tecnici Sanitari di Radiologia Medica e delle Professioni Sanitarie Tecniche, della Riabilitazione e della Prevenzione della Provincia di Bologna (d'ora in poi per brevità **Ordine Dei TSRM E PSTRP Di Bologna**), con sede in Galleria Ugo Bassi 1, 40121 Bologna (Bo), in persona del Presidente del Consiglio Direttivo pro tempore Dr. Giancarlo Lucchi, **Titolare del trattamento dei dati personali**, in ottemperanza alla prescrizione di cui all'art. 13, comma 6, del D.lgs. 24/2023, ha effettuato **una Valutazione d'impatto sulla protezione dei dati personali** (di seguito per brevità "**DPIA**") in relazione al trattamento dei dati personali che sarà effettuato dal Titolare per la gestione delle segnalazioni scritte in materia di "Whistleblowing" di cui al d.lgs. 24/2023, tramite **l'utilizzo della piattaforma informatica crittografata di Whistleblowing,** le cui caratteristiche saranno di seguito dettagliatamente indicate.

La 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 metodo seguito nella predisposizione della presente DPIA si base sullo strumento predisposto dalla Autorità di controllo francese, ossia la *Commission Nationale de l'Informatique et des libertés "CNIL"* e sulla base della documentazione tecnica ricevuta dalla società Whistleblowing Solutions I.S. S.r.l., fornitrice della piattaforma.

VALUTAZIONE DI IMPATTO PER LA PROTEZIONE DEI DATI PERSONALI

1. CONTESTO (*questa sezione contiene una descrizione complessiva del trattamento in questione)*

a) Panoramica del trattamento (questa sezione permette di individuare e presentare l'oggetto dell'analisi)

Qual è il trattamento in considerazione?

Il trattamento consiste nella gestione delle segnalazioni in forma scritta previste dal d.lgs. 24/2023 "*Whistleblowing*" e dalle Linee guida ANAC.

La gestione delle segnalazioni avviene attraverso una **piattaforma informatica crittografata**, fornita da Transparency International Italia e Whistleblowing Solutions attraverso il progetto WhistleblowingIT. La piattaforma utilizza **GlobaLeaks**, il principale software open-source per il whistleblowing. **Questo strumento garantisce, da un punto di vista tecnologico, la riservatezza della persona segnalante, dei soggetti menzionati nella segnalazione e del contenuto della stessa**.

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.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità sono così delineate:

- **Titolare del Trattamento**: Ordine dei TSRM e PSTRP di Bologna;
- **Gestore delle segnalazioni e Custode dell'Identità**: il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), anche Referente privacy, è stato nominato quale Soggetto Autorizzato dal Titolare del Trattamento a trattare i dati relativi alle segnalazioni e Custode dell'identità del Segnalante (doc. 1). Il RPCT potrà avvalersi di altri soggetti autorizzati al trattamento che abbiano preventivamente ricevuto la nomina come soggetti autorizzati e le relative istruzioni (doc. 2);
- **Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing**: Whistleblowing Solutions (doc. 3);
- **Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS):** Seeweb
- **Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing:** Transparency International Italia

Ci sono standard applicabili al trattamento?

Il contesto normativo di riferimento richiede conformità al:

● D. Lgs. n. 24/2023

● Direttiva (Ue) 2019/1937 (Whistleblowing)

- Linee Guida ANAC

● General Data Protection Regulation - 2016/679 (GDPR)

Il Responsabile del trattamento adotta misure progettate in aderenza allo **standard internazionale ISO37002:2021** in materia di gestione dei processi di whistleblowing. 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

b) Dati, processi e risorse di supporto

Quali sono i dati trattati?

a) *dati personali comuni,* quali: dati *anagrafici* (ad es. nome, cognome, data e luogo di nascita) e *dati di contatto* (es. numero telefonico fisso e/o mobile, indirizzo postale/e-mail) del Segnalante (nel caso di Segnalazioni non anonime) nonché di eventuali persone coinvolte e/o menzionate nella Segnalazione, e/o *dati comuni* dei c.d. Facilitatori, come definiti dalla Procedura Whistleblowing;

b) *Categorie particolari* di dati personali cui all'art. 9 del G.D.P.R., qualora inserite nella segnalazione.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

1) Attivazione della piattaforma;

2) Configurazione della piattaforma;

3) 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

Quali sono le risorse di supporto ai dati?

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 (Questa sezione permette di generare lo schema di adeguamento secondo i principi di protezione dei dati personali)

a) Proporzionalità e necessità

Gli scopi dei trattamenti sono specifici, espliciti e legittimi?

Si, previsti dalla normativa.

Quali sono le basi legali che rendono lecito il trattamento?

D.Lgs. n. 24 del 2023, Linee Guida ANAC, General Data Protection Regulation - 2016/679 (G.D.P.R.) indicate nell'informativa privacy e nel registro delle attività di trattamento ai sensi dell'art. 30 G.D.P.R.

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

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 sono esatti e aggiornati?

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. In caso di aggiornamento di altri dati oggetto della segnalazione, il segnalante potrà utilizzare la modulistica prevista per l'esercizio dei diritti di cui agli artt- 15 -21 G.D.P.R.

Qual è il periodo di conservazione dei dati?

I dati personali sono conservati per il tempo strettamente necessario al trattamento della segnalazione e, comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, come prescritto dall'art. 14 del D.lgs. n. 24/2023.

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

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

Come sono informati del trattamento gli interessati?

I soggetti interessati sono informati sul trattamento dei dati personali mediante apposita informativa redatta ai sensi dell'art. 13 G.D.P.R. (doc. n. 4) e pubblicata sul sito web nella sezione dedicata al *"Whistleblowing"*.

Ove applicabile: come si ottiene il consenso degli interessati?

Per le ipotesi specificamente previste dal d.lgs. 24/2023 (art. 12, commi 2 e 5, e art. 14, commi 2 e 4), il consenso è acquisito mediante moduli appositamente predisposti e menzionati nella procedura, nel rispetto della normativa in esame (doc. 5).

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

Il diritto di portabilità non si applica ai trattamenti effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 20, comma 3 GDPR), fattispecie in cui ricade il trattamento in oggetto.

Il Titolare è dotato di una procedura generale per l'esercizio dei diritti di cui agli artt-15-21 G.D.P.R.

Per tale tipo di trattamento, in conformità con le disposizioni di cui al d.lgs. n. 24/2003 che richiedono la massima attenzione nella tutela e protezione dell'identità del Segnalante, il Titolare ha ritenuto di dover adottare una procedura ad hoc gestita unicamente dal RPCT (doc. n. 6) e/o da soggetti espressamente autorizzati. L'esercizio dei diritti può avvenire mediante apposito modulo pubblicato sul sito web dell'ente secondo la specifica procedura adotttata.

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

Come indicato al punto precedente.

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

Come sopra.

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

Si, mediante sottoscrizione di un Accordo ai sensi dell'art. 28 G.D.P.R. (doc. n. 3)

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

N/A. Non viene effettuato alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea.

3. RISCHI (questa sezione permette di valutare i rischi per la riservatezza, alla luce delle misure esistenti o pianificate)

Il contesto in esame è caratterizzato da elevati rischi per i diritti e le libertà degli interessati che possono riguardare:

a) il rischio di impatto per la perdita di riservatezza dell'identità;
b) il rischio di impatto per la perdita di disponibilità dei dati

Entrambi i rischi risultano adeguatamente mitigati dall'adozione delle misure di sicurezza tecniche e organizzative indicate in questo paragrafo 3 e nei precedenti. Si ritiene infatti, anche sulla base delle

indicazioni di cui alle Linee Guida ANAC, che il ricorso ad una piattaforma **informatica crittografata,** con le caratteristiche di seguito specificate, costituisca una misura adeguata a dare attuazione, fin dalla progettazione e per impostazione predefinita, al principio di integrità e riservatezza dei dati dei segnalanti.

Il rischio di perdita di riservatezza dell'identità del segnalante e/o di disponibilità dei dati deve quindi ritenersi basso alla luce della piattaforma adottata.

a) Misure esistenti o pianificate (questa sezione permette di indicare le misure - esistenti o pianificate - che contribuiscono alla sicurezza dei dati)

1. 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

2. 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.

3. 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.

4. 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.

5. 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

6. 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.

7. Manutenzione

Il Responsabile del trattamento garantisce una 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.

8. 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.

9. 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.

10. Gestione degli incidenti di sicurezza e delle violazioni dei dati personali

Il Titolare è dotato di un proprio regolamento per la gestione dei data breach. Anche Whistleblowing Solutions, Responsabile del trattamento dei dati personali, ha definito una procedura per la gestione delle violazioni dei dati personali.

11. Lotta contro il malware

I computer del personale del Titolare, del Responsabile del trattamento e e dei sub-responsabili nominati eseguono firewall e antivirus peridici.

12. Predisposizione procedura per la gestione delle segnalazioni

Come da procedura allegata (doc. n. 7)

13. Cancellazione dati ultronei

Come da indicazioni normative e procedura di gestione delle segnalazioni

14. Contratto con il responsabile del trattamento ex art. 28 GDPR

Si

15. Nomina incaricati del trattamento ex artt. 29 GDPR e 2-quaterdecies Codice privacy

Si

16. Formazione

Si in materia di protezione dei dati personali e whistleblowing.

b) Accesso illegittimo ai dati (analizzare le cause e le conseguenze di accesso illegittimo ai dati, stimandone la gravità e la probabilità)

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Rischio ritorsioni in caso di divulgazione dell'identità del segnalante

Quali sono le principali minacce che potrebbero concretizzare il rischio?

• errata gestione della procedura;

• violazione istruzioni sul trattamento;

• conservazione dei dati oltre il tempo necessario al perseguimento della finalità per la quale sono stati raccolti;

• accesso non autorizzato ai dati o diffusione incontrollata;

• intrusioni informatiche.

Quali sono le fonti di rischio?

• fonti interne umane - soggetti che avrebbero interesse ad ottenere le informazioni riservate e soggetti che gestiscono le informazioni;

• fonti esterne umane - soggetti che avrebbero interesse ad ottenere le informazioni riservate e responsabili del trattamento;

• non umane: di tipo ambientale e/o informatico.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Tutte le misure sopra espressamente indicate contribuiscono a mitigare il rischio.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate (indefinito; trascurabile; limitato; importante; massimo)?

Alla luce delle misure pianificate, il rischio appare limitato.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate (indefinito; trascurabile; limitato; importante; massimo)?

Alla luce delle misure pianificate, la probabilità del rischio appare limitata.

c) Modifiche indesiderate (analizzare le cause e le conseguenze di modifiche indesiderate dei dati, e stimare la gravità e la probabilità dell'evento)

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Rischio ritorsioni in caso di divulgazione dell'identità del segnalante

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Vedere risposta al medesimo quesito lett. b.

Quali sono le fonti di rischio?

Vedere risposta al medesimo quesito lett. b.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Tutte quelle indicate.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate (indefinito; trascurabile; limitato; importante; massimo)?

Limitato

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

Limitato

D) Perdita di dati

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Vedere risposta al medesimo quesito per lett. b.

Quali sono le fonti di rischio?

Vedere risposta al medesimo quesito per lett. b.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Vedere sopra, risposta al medesimo quesito per lett. b.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate (indefinito; trascurabile; limitato; importante; massimo)?

Vedere sopra, risposta al medesimo quesito per lett. b.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate (indefinito; trascurabile; limitato; importante; massimo)?

Vedere sopra, risposta al medesimo quesito lett. b.

e) Panoramica dei rischi (questa visualizzazione permette una panoramica globale e sintetica degli effetti prodotti dalle misure sulle componenti di rischio che esse contribuiscono a mitigare).

Alla luce delle misure adottate e delle caratteristiche della piattaforma scelta, di cui si allega la scheda tecnica fornita dal Responsabile del trattamento (doc. n. 8), si ritiene che il rischio possa ritenersi non elevato e stimato come basso.

4. CONVALIDA (questa sezione permette di preparare e formalizzare la convalida DPIA)

a) Piano d'azione

La piattaforma informatica crittografata, le misure di sicurezza tecniche e organizzative garantiscono nel complesso la riservatezza della persona segnalante, dei soggetti menzionati nella segnalazione e del contenuto della stessa. Resta fermo che le misure indicate saranno oggetto di implementazione sulla base dell'evoluzione tecnologica.

c) Pareri di DPO/RPD e interessati

Parere del DPO/RPD

Tenuto conto di quanto sin qui rappresentato e alla luce delle misure tecniche e organizzative predisposte e alle garanzie di affidabilità del Responsabile del trattamento dei dati, il DPO ritiene che il trattamento possa essere effettuato mediante l'utilizzo della piattaforma individuata.

5. VALIDAZIONE DELLA PIA

Il sottoscritto Dott. Filippo Mosconi, in qualità di Referente privacy dell'ente, acquisito il parere del DPO favorevole all'utilizzo della piattaforma su indicata, sottopone la DPIA all'approvazione del Consiglio direttivo per la sua validazione.

Si allegano:

1) Atto di nomina RPCT come soggetto autorizzato ad accedere alla piattaforma e al trattamento dei dati personali e istruzioni;
2) Atto di nomina soggetti autorizzati;
3) Accordo ai sensi dell'art. 28 del GDPR avente ad oggetto la designazione di Whistleblowing Solutions I.S. S.r.l. come Responsabile del trattamento;

4) Informativa privacy,
5) Moduli consenso;
6) Procedura esercizio diritti e allegati (registro + modulo);
7) Procedura gestione segnalazioni;
8) Scheda tecnica fornita dal Responsabile del trattamento.

Bologna, 20 Marzo 2024

Il Referente Privacy

Dott. Filippo Mosconi

Il Consiglio Direttivo dell'Ordine dei TSRM E PSTRP Di Bologna, riunitosi in data 19/03/2024 in persona del legale rappresentante pro tempore, **approva e valida la presente DPIA.**

Il Presidente dell'Ordine TSRM-PSTRP di Bologna

Dott. Giancarlo Lucchi