DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Art. 35 GDPR GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING

1. PREMESSA

Il Regolamento UE n. 679/2016 (GDPR), all'art. 35, impone al Titolare del trattamento di effettuare una Valutazione di Impatto (di seguito "DPIA") qualora un trattamento "possa presentare un rischio elevato" per i diritti e le libertà delle persone fisiche. Lo svolgimento della DPIA nei casi dubbi è sempre raccomandato, in quanto la valutazione in esame è uno strumento che permette di realizzare e dimostrare la conformità del trattamento svolto alle norme del GDPR. L'art. l'art. 13, comma 6, del D. Lgs. 24/2023 (Decreto Whistleblowing) prevede espressamente per i soggetti chiamati a dotarsi di un canale interno per la raccolta e la gestione delle segnalazioni (Titolari del Trattamento) la necessità di procedere con una valutazione d'impatto sulla protezione dei dati, al fine di individuare e applicare le necessarie misure tecniche per garantire la sicurezza dei dati personali oggetto di trattamento.
Si tratta di 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.
La presente DPA è redatta in base alle disposizioni contenute nell'art. 35 del GDPR ed è, in ogni caso, effettuata tenendo conto dei principi e dei diritti fondamentali stabiliti dalla legge che devono essere rispettati e tutelati e non possono essere soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi; dei rischi per la privacy dei soggetti interessati che devono essere minimizzati mediante l'utilizzo di idonei strumenti tecnici di controllo e gestioni.
Il presente documento sarà aggiornato alla luce delle eventuali modifiche normative, organizzative o tecniche che potranno interessare nel tempo il trattamento oggetto di valutazione.

2. RIFERIMENTI NORMATIVI

Al trattamento in materia di segnalazioni interne si applicano le seguenti normative:

- Regolamento Europeo in materia di protezione dei dati personali 2016/679 (di seguito "GDPR");
- D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018 (di seguito "Codice Privacy");
- Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione delle possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 del 4 ottobre 2017 (WP 248);
- Direttiva (UE) del Parlamento Europeo e del Consiglio del 23 ottobre 2019 n. 1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (whistleblowing);
- D. Lgs 10 marzo 2023, n. 24, in 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 ("Whistleblowing").

3. CONTESTO

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi del D.lgs. n. 24/2023. Segnatamente, il trattamento riguarda la raccolta e successiva gestione dei dati personali del Segnalante, del Segnalato e delle eventuali persone menzionate nella segnalazione effettuata utilizzando il canale interno predisposto dalla Società, come descritto nella Procedura Whistleblowing adottata dalla Società.

I dati degli interessati (segnalanti, segnalati ed eventuali altri soggetti terzi coinvolti) possono essere forniti dal medesimo interessato, oppure da terzi (è il caso, a titolo esemplificativo, dei dati della persona segnalata che sono forniti dal segnalante e dei dati acquisititi nell'ambito dell'attività istruttoria, svolta dal Responsabile della gestione del canale di segnalazione interno, cd. Responsabile Whistleblowing).

Le finalità perseguite con il trattamento in questione riguardano:

- la gestione delle segnalazioni ricevute,
- l'accertamento dei fatti oggetto delle stesse;
- l'adozione dei conseguenti provvedimenti e delle azioni di rimedio.

Il sistema adottato dalla Società prevede la possibilità per il Segnalante di effettuare segnalazioni in forma scritta attraverso l'utilizzo di un applicativo informativo denominato "WHISTLESBLOW.IT", accessibile attraverso apposito link pubblicato sulla pagina web del sito aziendale: https://whistlesblow.it/c/gb-thermae-hotel/1. La piattaforma in questione permette al Segnalante di procedere con una segnalazione anonima (non è prevista la compilazione di campi che richiedono i dati identificativi) oppure fornire le proprie generalità (nome, cognome, data e luogo di nascita), il ruolo ricoperto nell'ambito dell'azienda e indicare eventuali dati di contatto (numero di telefono, indirizzo mail, ecc.). È poi possibile effettuare la scelta circa le modalità attraverso le quali presentare una segnalazione. La Società ha individuato il soggetto deputato alla gestione del processo di Whistleblowing in un consulente esterno, Avv. Claudio Calvello, del Foro di Padova, c/o Studio Legale Calvello di Abano Terme (PD) (di seguito, "Gestore").

4. RUOLI PRIVACY – RESPONSABILITA' CONNESSE AL TRATTAMENTO

Nella seguente tabella vengono riportati i soggetti coinvolti nel trattamento dei dati personali oggetto della presente DPIA, con indicazione dei rispettivi ruoli privacy rivestiti.

TITOLARE DEL TRATTAMENTO	G.B. THERMAE HOTELS S.R.L. (C.F. 00220810287), con sede in Abano Terme (PD) Via Flacco n. 99, CAP 35031
RESPONSABILE DEL TRATTAMENTO (Gestore della Segnalazione)	AVV. CLAUDIO CALVELLO (C.F. CLVCLD65B22A001L) c/o STUDIO LEGALE CALVELLO, con sede in Abano Terme (PD) – Via Previtali n. 30, CAP 35031
SUB RESPONSABILE DEL TRATTAMENTO (Fornitore Piattaforma)	HOLDINGS SHAKE DI PISARONI ALBERTO (C.F. PSRLRT95R24G337P), con sede Busseto (PR) Via Mozart n. 9, CAP 43011 Il Fornitore della Piattaforma può accedere unicamente ai dati crittografati e solo al fine di garantire i servizi di assistenza, manutenzione e aggiornamento del sistema informatico
AUTORIZZATI AL TRATTAMENTO	Organi sociali e/o Responsabili di Funzione ai quali vengono comunicati i risultati delle indagini effettuate a seguito della ricezione di una segnalazione

5. DATI TRATTATI

La piattaforma adottata dalla Società, attraverso una procedura di compilazione guidata, consente al Segnalante di fornire solo le informazioni necessarie alla comprensione dei fatti oggetto di segnalazione e alla successiva verifica circa l'ammissibilità e la fondatezza della stessa. I dati personali non utili al trattamento di una specifica segnalazione non vengono raccolti o, se raccolti accidentalmente, vengono cancellati immediatamente a cura del Gestore della segnalazione. I dati personali che possono essere oggetto del trattamento possono essere:

- **Dati anagrafici e dati di contatto dei "soggetti segnalanti" e delle "persone coinvolte"**, quali a titolo esemplificativo: nome, cognome, tipo di rapporto intercorrente con la Società, inquadramento, ruolo, qualifica, contatto telefonico, indirizzo mail;

- **Informazioni che il Segnalante ha fornito per rappresentare i fatti descritti nella segnalazione**. In considerazione del fatto che la piattaforma prevede alcuni spazi aperti, attraverso cui il Segnalante può procedere liberamente alla descrizione della violazione oggetto di segnalazione (descrizione dei fatti e descrizione degli autori della violazione, unitamente alla possibilità di caricare documentazione idonea a suffragare i fatti segnalati), non è possibile escludere a priori che tra i dati raccolti possano figurare anche dati particolari (art. 9 GDPR) o relativi a condanne penali e reati (art. 10 GDPR).
- **Dati personali particolari dei "soggetti segnalanti" e delle "persone coinvolte"**, quali, a titolo esemplificativo, i dati relativi alla salute, all'appartenenza sindacate);
- **Dati giudiziali** (es: condanne penali) dei "soggetti segnalanti" e delle "persone coinvolte".

6. CICLO DI VITA DEL TRATTAMENTO DEI DATI

Mediante utilizzo della piattaforma:

- attivazione e configurazione della piattaforma

- utilizzo della piattaforma – invio delle segnalazioni da parte dei segnalanti ed accesso alle stesse da parte dei soggetti autorizzati

- dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.

7. ASSET UTILIZZATI – RISORSE A SUPPORTO DEI DATI

La Società, in qualità di Titolare del Trattamento, ha individuato le seguenti risorse:

- PORTALE WHISTLEBLOWING – "WHISTLESBLOW.IT", sito accessibile con qualunque dispositivo (computer, iPad, smartphone) senza necessità di installazione di software/app aggiuntivo.

8. NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO – PRINCIPI FONDAMENTALI

REQUISITI	**CONFORMITA'/NON CONFORMITA'**
I DATI PERSONALI SONO RACCOLTI PER FINALITÀ DETERMINATE, ESPLICITE E LEGITTIME?	Il trattamento è finalizzato esclusivamente alla gestione della segnalazione ed all'adempimento

	degli obblighi derivanti dalla normativa vigente in materia di Whistleblowing.
I DATI PERSONALI RACCOLTI SONO PERTINENTI E LIMITATI A QUANTO NECESSARIO RISPETTO ALLE FINALITÀ PER I QUALI SONO TRATTATI?	I dati personali raccolti sono quelli espressamente necessari alla gestione della segnalazione, come previsto dall'art. 12 del D. Lgs. 24/2023. Il rispetto del principio di minimizzazione dei dati è assicurato dall'utilizzo della Piattaforma Whistleblowing che, attraverso lo specifico form presente nell'applicativo, permette la raccolta delle sole informazioni necessarie ai fini della gestione della segnalazione. La Società si è dotata di specifico atto organizzativo (Procedura Whistleblowing) che prevede che le informazioni raccolte accidentalmente che, a parere del Gestore, non sono utili al trattamento della specifica segnalazione sono immediatamente cancellate a cura dello stesso Gestore.
I DATI PERSONALI TRATTATI SONO ESATTI E AGGIORNATI?	Il trattamento dei dati personali relativi alle segnalazioni sono aggiornati costantemente giacché i soggetti incaricati di ricevere e gestire le segnalazioni ne verificano preliminarmente la corrispondenza a verità e li aggiornano, se necessario, nel corso dell'attività istruttoria.
È STATA CORRETTAMENTE INDIVIDUATA LA BASE GIURIDICA LEGITTIMANTE IL TRATTAMENTO?	Il trattamento è necessario per l'adempimento di un obbligo di legge (come previsto dal D.Lgs. 24/2023) a cui è tenuto il Titolare (Art. 6.1. lett. c) GDPR).
QUAL È IL PERIODO DI CONSERVAZIONE DEI DATI?	Le segnalazioni interne 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'art. 14 D.Lgs. 24/2023.
I principi di necessità e proporzionalità risultano correttamente rispettati; sul punto non si rilevano inadeguatezze del sistema adottato dalla Società.	

9. MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

COME SONO INFORMATI DEL TRATTAMENTO GLI INTERESSATI?	Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13 e 14 GDPR. L'informativa viene resa disponibile attraverso la pubblicazione sul sito internet della Società, nella sezione dedicata al Whistleblowing.
E' PREVISTA LA RICHIESTA DI CONSENSO DEL SOGGETTO INTERESSATO/SEGNALANTE?	Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita di un consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (art. 6.1 lettera c) GDPR). Ogniqualvolta invece sia richiesto il consenso del segnalante, quest'ultimo dovrà, tramite piattaforma, prestare il proprio consenso espresso alla comunicazione dei dati ai sensi degli artt. 6.1. lettera a) e 7 del GDPR.
COME FANNO GLI INTERESSARI A ESERCITARE I LORO DIRITTI PREVISTI DAGLI ARTT. 15 SS GDPR?	Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss del GDPR attraverso l'indirizzo di posta elettronica dedicato, nei limiti di cui all'art. 2-undecies GDPR.
GLI OBBLIGHI DEI RESPONSABILI DEL TRATTAMENTO SONO DEFINITI CON CHIAREZZA E DISCIPLINATI DA UN CONTRATTO?	L'Avv. Claudio Calvello, in qualità di gestore delle segnalazioni Whistleblowing, è Responsabile del Trattamento ai sensi dell'art. 28 GDPR. La Società fornitrice della piattaforma per le segnalazioni Whistleblowing agisce in qualità di Sub-responsabile al trattamento.

	Tutte trattano i dati personali per conto del Titolare.
IN CASO DI TRASFERIMENTO DI DATI AL DI FUORI DELL'UNIONE EUROPEA, I DATI GODONO DI UNA PROTEZIONE EQUIVALENTE?	Per questa tipologia di trattamento non è previsto un trasferimento di dati personali fuori dall'Unione Europea.

10. MISURE ESISTENTI

ARCHITETTURA DI SISTEMA	La piattaforma è installata all'interno di una macchina virtuale con sistema operativo "Ubuntu 22.04 LTD" presso il provider della Società fornitrice della piattaforma AWS (Amazon Web Services) e più precisamente collocata presso il datacenter di Milano (MI).
SOFTWARE IMPIEGATO	L'applicativo fornito in modalità SaaS (SoMware as a Service) è sviluppato in-house con tecnologia PHP utilizzando il framework Laravel.
ARCHITETTURA DI RETE	Tutta l'infrastruttura è contenuta in una singola macchina virtuale con accessi pubblici circoscritti alle porte HTTP e HTTPS. Esiste un accesso privilegiato alla console di manutenzione SSH che può provenire solo da indirizzi IP pubblici specifici, ovvero quelli dell'amministratore di sistema nominato. Tutti i moduli sono configurati per non generare log (registri di attività) contenenti informazioni lesive della privacy o dell'anonimato del segnalante.
CRITTOGRAFIA	In caso di utilizzo della piattaforma, l'applicativo implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing. In particolare, ogni informazione in transito viene protetta da protocollo TLS 1.2 con cifrature AES128/SHA256.

CONTROLLO DEGLI ACCESSI LOGICI	L'accesso applicativo alla piattaforma è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta l'utilizzo di precedenti password.
TRACCIABILITA'	Viene utilizzato un meccanismo di audit minimale che memorizza un identificativo dell'operatore autorizzato e la data/ora di modifica/creazione delle informazioni presente nel database. Le operazioni effettuate dai segnalanti hanno un identificativo completamente anonimizzato (auto generato) e legato al singolo ticket e non alla persona del segnalante.
ARCHIVIAZIONE	L'applicativo ha completo ed esclusivo controllo della base dati ed implementa al suo interno le logiche di data retention e cancellazione sicura previste dalle policy normative. Tutte le segnalazioni e i relativi dati salvati vengono cancellati automaticamente dopo massimo 5 anni dalla data di apertura.
GESTIONE DELLE VULNERABILITA' TECNICHE	L'amministratore di sistema incaricato riceve ticket di sicurezza riguardanti i moduli software in uso dall'infrastruttura ed è in grado di intervenire tempestivamente, per poter mitigare eventuali vulnerabilità critiche o malfunzionamenti del servizio fornito.
BACKUP	È presente un backup dell'intero sistema effettuato ogni giorno alle ore 04:00 GMT+1.
MANUTENZIONE	L'amministratore di sistema incaricato effettua interventi almeno trimestrali (in assenza di criticità elevate) per allineare le versioni del software in uso (sia di sistema, che applicativo) con le ultime patch migliorative stabili pubblicate dai rispettivi fornitori. I lavori di manutenzione

	verranno sempre effettuati in orario notturno, tra le 01.00 e le 06.00 GMT+1.
SICUREZZA DEI CANALI INFORMATICI	Tutte le connessioni sono protette tramite protocollo TLS 1.3.
SICUREZZA DELL'HARDWARE	Si rinvia alle protezioni di sicurezza adottate dal provider AWS (Amazon Web Services), collocata presso il datacenter di Milano (MI).
POLITICA DI TUTELA PRIVACY	Il prodotto è conforme con le normative GDPR in materia, applicando misure idonee a proteggere i dati personali da accessi non autorizzati, modifiche, danni e distruzione. In particolare, gli amministratori e gli sviluppatori del prodotto operano in contesti di sicurezza conformi alle linee guida in materia, con firewall al passo con le minacce informatiche di oggi.
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 dalla Società in conformità a quanto prescritto dagli artt. 33- 34 del GDPR.
VIGILANZA SULLA PROTEZIONE DEI DATI	Vigilanza svolta da DPO/Comitato Privacy/funzioni incaricate dal Titolare del trattamento (a seconda di quanto definito nell'organigramma privacy aziendale)

11. ANALISI DEI RISCHI

- METODOLOGIA

Il livello di impatto è sempre correlato alle conseguenze che una violazione del trattamento e della sicurezza dei dati personali potrebbe comportare per gli interessati, i cui dati sono stati oggetto di violazione.

Di seguito quattro livelli di impatto:

LIVELLO DI IMPATTO	**DESCRIZIONE**
Basso	I soggetti possono essere potenzialmente sottoposti a disagi significativi, superabili senza particolari problemi (a titolo esemplificativo ma non esaustivo: il dover perdere un po' più di tempo per reinserire le informazioni...)
Medio	I soggetti possono essere potenzialmente sottoposti a disagi significativi, superabili ma con qualche difficoltà (a titolo esemplificativo ma non esaustivo: il dover affrontare costi aggiuntivi, problemi ad accedere a servizi aziendali...)
Alto	I soggetti possono essere potenzialmente sottoposti a conseguenze significative, che probabilmente sapranno superare ma con grande difficoltà (a titolo esemplificativo ma non esaustivo: in caso di appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà...)
Molto Alto	I soggetti possono essere potenzialmente sottoposti a conseguenze significative, o addirittura irreversibili, che potrebbero non essere in grado di superare (a titolo esemplificativo ma non esaustivo: trovarsi nell'incapacità di lavorare...)

La valutazione dell'impatto è condotta esaminando le specificità dell'operazione di trattamento.

I parametri considerati sono i seguenti:

- la tipologia dei dati trattati: certi dati, se violati, possono impattare più di altri sull'individuo (ad es., dati sanitari, di appartenenza politica, di residenza o finanziari);

- il volume di dati trattati, sia dal punto di vista della quantità che dal punto di vista della durata temporale;

- le caratteristiche peculiari del Titolare del trattamento e degli interessati.

Nella valutazione dell'impatto sono esaminati altresì i possibili effetti collaterali secondari (sui diritti e le libertà delle persone).

La seguente valutazione consente di ottenere i diversi livelli di impatto per ciascuna delle seguenti tipologie di violazioni:

	TIPOLOGIA DI VIOLAZIONE	**LIVELLO DI GRAVITA' (tra i seguenti: basso, medio, alto, molto alto)**
1	PERDITA DI RISERVATEZZA → Valutare l'impatto che una divulgazione non autorizzata dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo	**Alto**
2	PERDITA DI INTEGRITA' → Valutare l'impatto che un'alterazione non autorizzata dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo	**Alto**
3	PERDITA DI DISPONIBILITA' → Valutare l'impatto che una distruzione o perdita non autorizzata dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo	**Medio**

- **DEFINIZIONE DELLE POSSIBILI MINACCE**

Di seguito vengono prese in considerazione le minacce correlate al contesto complessivo del trattamento dei dati personali e vengono valutare ed esaminate la loro probabilità di accadimento.

Le diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati sono quattro e sono di seguito identificate:

A) Risorse di rete e tecniche (hardware e software);

B) Processi / procedure relativi all'operazione di trattamento dei dati;

C) Parti e persone coinvolte nell'operazione di trattamento;

D) Settore di operatività e scala del trattamento.

Ciò premesso, le predette categorie vengono esaminate separatamente.

A) Risorse di rete e tecniche (hardware e software)

Qualche parte del trattamento dei dati personali viene effettuata tramite Internet?	**SI**
È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	**SI**
Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	**SI**
Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	**NO**
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	**NO**

Pertanto, il livello di probabilità registrato è (tra basso, medio e alto): MEDIO.

B) Processi / procedure relativi all'operazione di trattamento dei dati

I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	**NO**
L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	**NO**
I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	**NO**
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	**NO**

Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file log di registro?	**SI**

Pertanto, il livello di probabilità registrato è (tra basso, medio e alto): BASSO.

C) Parti/Persone coinvolte nel trattamento dei dati personali

Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	**NO**
Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (Responsabile del trattamento)?	**SI**
Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	**NO**
Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	**NO**
Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	**NO**

Pertanto, il livello di probabilità registrato è (tra basso, medio e alto): BASSO.

D) Settore di operatività e Scala di trattamento

Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	**SI**
La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	**NO**
Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del tuo sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	**NO**

Un'operazione di elaborazione riguarda un grande volume di individui e/o di dati personali?	**NO**
Esistono best practices di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente messe in atto?	**NO**

Pertanto, il livello di probabilità registrato è (tra basso, medio e alto): BASSO.

- **VALUTAZIONE DELLE PROBABILITÀ DI OCCORRENZA DELLE MINACCE PER AREA:**

AREA DI VALUTAZIONE	**PROBABILITA'**	
	LIVELLO	**PUNTEGGIO**
A) RISORSE DI RETE E TECNICHE	Basso	1
	MEDIO	**2**
	Alto	3
B) PROCESSI/PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO	**BASSO**	**1**
	Medio	2
	Alto	3
C) PARTI/PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	**BASSO**	**1**
	Medio	2
	Alto	3
D) SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	**BASSO**	**1**
	Medio	2
	Alto	3

- VALUTAZIONE COMPLESSIVA DELLA MINACCIA

SOMMA DEI PUNTEGGI DELLE 4 AREE DI VALUTAZIONE	**LIVELLO DI PROBABILITA' DEL VERIFICARSI DELLA MINACCIA**
4 - 5	Basso
6 - 8	Medio
9 - 12	Alto

→ VALUTAZIONE DEL RISCHIO: BASSO

12. PARERE DELLE PARTI INTERESSATE

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

13. PARERE DPO

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 conforme al dettato normativo.

14. CONCLUSIONI

Alla luce dell'analisi sull'impatto dei rischi valutati, con particolare attenzione, nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono rischi di impatto sui diritti e libertà dei soggetti interessati con stima a valore basso, ritenuto accettabile dall'organizzazione in relazione ai parametri oggettivi considerati. Si ritiene che il trattamento dei dati in oggetto presenti un grado di rischio sui diritti e libertà dell'interessato sussumibile nei parametri accettabili e, per l'effetto, va esente da una consultazione preventiva all'Autorità Garante.