DATA PROTECTION IMPACT ASSESSMENT (DPIA)
Art. 35 GDPR

GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING

REVISIONI DEL DOCUMENTO

Data attività	Commento	Validazione
dicembre 2023	Redazione Data Protection Assessment (DPIA)	

SOMMARIO

1. PREMESSA

Il GDPR 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.

Scopo del presente documento, pertanto, è di delineare il quadro delle misure di sicurezza - organizzative, tecniche e legali - adottate e da adottare per il trattamento dei dati personali effettuato da GAB TAMAGNINI s.r.l. (di seguito "Società").

La presente DPIA è redatta in base alle disposizioni contenute nell'art. 35 del GDPR e alle linee guida dell'EDPB (European Data Protection Board), già WP29, n. 248 del 4.10.2017.

Il presente documento sarà aggiornato alla luce delle modifiche normative, organizzative o tecniche che potranno interessare nel tempo il trattamento oggetto di valutazione.

2. RIFERIMENTI NORMATIVI

- 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 oggetto di DPIA 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.

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 "**PORTALE WHISTLEBLOWING**", accessibile attraverso apposito link pubblicato sulla pagina web del sito aziendale: https://www.gabtamagnini.it/whistleblowing.

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 e cognome) e indicare eventuali dati di contatto (numero di telefono, indirizzo mail, ecc.).

La Società ha individuato il soggetto deputato alla gestione del processo di Whistleblowing in un consulente esterno, Avv. Emanuela Arduini c/o Studio L&E – Legal and Engineering di Reggio Emilia (di seguito, "Gestore").

4. RUOLI PRIVACY

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	GAB TAMAGNINI s.r.l. Reggio Emilia, Via G. Oberdan 7
RESPONSABILE DEL TRATTAMENTO (Gestore della Segnalazione)	Avv. Emanuela Arduini c/o Studio L&E - Legal and Engineering Via F.lli Cervi 59, Reggio Emilia Link: Studio L&E | Legal and Engineering
RESPONSABILE DEL TRATTAMENTO (Fornitore Piattaforma)	TeamSystem S.p.A. Via Sandro Pertini 88, Pesaro. 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
SUB-RESPONSABILI DEL TRATTAMENTO	Smart Flow Srl SB Corso Giuseppe Siccardi, 11 bis Torino Sito web: https://smart-flow.it

	Configurazione dei portali Whistleblowing, assistenza clienti Synesthesia Srl SB Corso Dante, 118, Torino Sito web: https://www.synesthesia.it Sviluppo e manutenzione software e hardware Host.it Corso Svizzera 185, Torino Sito web: https://host.it Servizio di hosting
AUTORIZZATI AL TRATTAMENTO	Organi sociali e 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, 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).

6. RACCOLTA DELLA SEGNALAZIONE

La segnalazione effettuata in forma scritta viene raccolta e gestita attraverso la Piattaforma informatica adottata dalla Società (Portale Whistleblowing), disponibile sul sito aziendale, al seguente link https://www.gabtamagnini.it/whistleblowing.

Per effettuare una nuova segnalazione, il Segnalante, dopo aver cliccato sul tasto "Invia una segnalazione", verrà rinviato alla pagina principale della Piattaforma nella quale è previsto, mediante la compilazione di un breve e semplice questionario, l'inserimento delle

informazioni inerenti alla segnalazione - relative alla descrizione del fatto e all'indicazione dei riferimenti di tempo e luogo – e l'allegazione di eventuale documentazione a sostegno di quanto descritto.

È bene precisare che il sistema non richiede la compilazione di campi volti alla raccolta di dati identificativi e/o di contatto, mostrando di prediligere, come impostazione base, la raccolta di segnalazioni anonime; ciò non esclude che il Segnalante possa identificarsi, fornendo di propria iniziativa le informazioni necessarie alla sua identificazione, riportando le stesse nel campo libero dedicato alla descrizione della condotta oggetto di segnalazione. Terminata la fase compilativa, attraverso il tasto "Invia", il Segnalante procede a inviare la segnalazione al sistema. La Piattaforma crea in automatico un codice numerico a 16 cifre che il Segnalante dovrà custodire e che in seguito potrà utilizzare per visualizzare la sua segnalazione e verificarne lo stato di lavorazione, per chattare con il Gestore e per inviare nuove informazioni e/o documentazione.

La Piattaforma non conserva alcuna copia del codice di segnalazione, pertanto, nel caso in cui il Segnalante smarrisse tale codice, non sarà possibile recuperarlo in alcun modo.

Anche se la modalità preferenziale indicata dal Titolare per procedere con una segnalazione è quella di utilizzare la citata Piattaforma, non è possibile escludere che la ricezione di segnalazioni avvenga anche attraverso canali o strumenti diversi. In questo caso, il rispetto della Procedura Whistleblowing adottata dalla Società garantisce comunque la riservatezza e la corretta conservazione della segnalazione.

Rispetto alla possibilità per il Segnalante di effettuare la segnalazione in forma orale, la Società ha previsto che questa possa avvenire mediante la richiesta di fissazione di un apposito incontro con il Gestore della Segnalazione. In tal caso, al fine di rendere tracciabile la raccolta della segnalazione, verrà redatto un verbale sottoscritto dal Segnalante e dal Gestore. Quest'ultimo garantisce la corretta conservazione della documentazione cartacea presso i propri locali.

Nel caso in cui la segnalazione arrivi a un soggetto diverso dal Gestore, la stessa dovrà essere immediatamente trasmessa all' organismo deputato alla ricezione delle segnalazioni per le opportune attività conseguenti, mantenendo la riservatezza in ordine all'identità del Segnalante e a tutte le informazioni contenute nella segnalazione.

7. GESTIONE DELLA SEGNALAZIONE

Il processo di gestione della segnalazione prevede le seguenti attività:

A. il Segnalante - sia nel caso in cui abbia reso nota la propria identità, sia nel caso in cui abbia effettuato una segnalazione anonima - potrà in ogni momento utilizzare le proprie credenziali di accesso generate all'invio della segnalazione originaria;

B. il Gestore della segnalazione mantiene le interlocuzioni con il Segnalante e può richiedere a quest'ultimo, ove lo ritenga necessario, ulteriori informazioni e/o documentazione. L'utilizzo della Piattaforma agevola tale attività, permettendo sia al Segnalante, sia al Gestore di richiedere l'integrazione di quanto originariamente trasmesso, tramite uno strumento sicuro;

C. una volta ricevuta la segnalazione e le eventuali necessarie integrazioni, il Gestore procede alla verifica della sussistenza dei requisiti essenziali per la valutazione di ammissibilità della stessa. Tale prima fase potrà portare all'archiviazione della segnalazione qualora la stessa risulti (i) avere a oggetto fatti/comportamenti/omissioni che non possono formare oggetto di segnalazione, (ii) manifestamente infondata per l'assenza di elementi di fatto idonei a giustificare ulteriori accertamenti, (iii) di contenuto generico, tale da non consentire la comprensione dei fatti, (iv) corredata da documentazione non appropriata o inconferente;

D. se la segnalazione viene valutata ammissibile, il Gestore avvia la fase di istruttoria interna, volta alla valutazione della fondatezza dei fatti oggetto di segnalazione. Nel corso di tale seconda fase, tenuto anche conto dell'oggetto della segnalazione, il Gestore può acquisire atti, documenti o informazioni da altri uffici della Società e coinvolgere terze persone tramite audizioni e richieste;

E. se la segnalazione, all'esito dell'istruttoria, risulta fondata, il Gestore procede a condividere i risultati dell'attività svolta con il Consiglio di Amministrazione/la Direzione competente, a seconda dell'oggetto della segnalazione e del soggetto coinvolto, affinché vengano adottati gli eventuali provvedimenti disciplinari/sanzionatori e le eventuali azioni di miglioramento. Nel caso in cui, invece, la segnalazione risulti infondata, il Gestore procede all'archiviazione motivata;

F. in ogni caso, il Gestore fornisce un riscontro, anche interlocutorio, al Segnalante entro tre mesi dalla data di ricezione della segnalazione e informa lo stesso circa l'esito delle indagini svolte.

8. TEMPO DI CONSERVAZIONE

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario alla gestione delle stesse. La Società ha comunque individuato il termine massimo di data retention, conformemente a quanto indicato dalla normativa in esame, nei 5 anni successivi alla comunicazione dell'esito finale della procedura di segnalazione.

I dati personali manifestamente non sono utili al trattamento di una specifica segnalazione eventualmente raccolti nella prima fase di creazione e invio della segnalazione e/o in occasione dei successivi contatti tra Gestore e Segnalante sono cancellati immediatamente a cura del Gestore.

9. ASSET UTILIZZATI

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

- PORTALE WHISTLEBLOWING, applicazione cloud accessibile con qualunque dispositivo (computer, iPad, smartphone) senza necessità di installazione di software/app aggiuntivo;

- Database di Host.it (all'interno dell'Unione Europea), sui quali vengono conservati i dati della Piattaforma

10. NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

REQUISITI	CONFORMITÀ/NON CONFORMITÀ
LE FINALITÀ DEL TRATTAMENTO SONO SPECIFICHE?	La Società, conformemente alle disposizioni dettate dalla normativa in materia di Whistleblowing, si è dotata di un sistema interno di segnalazione che garantisce, per impostazione predefinita, la protezione – sia in termini di riservatezza che di tutela da ritorsioni – dei soggetti segnalanti, allo scopo di favorire l'emersione e, conseguentemente, la prevenzione di rischi e situazioni pregiudizievoli per la Società stessa
I DATI PERSONALI SONO RACCOLTI PER FINALITÀ DETERMINATE, ESPLICITE E LEGITTIME?	I dati vengono raccolti e trattati al solo fine di gestire e dare seguito alle segnalazioni ricevute
I DATI PERSONALI RACCOLTI SONO PERTINENTI E LIMITATI A QUANTO NECESSARIO RISPETTO ALLE FINALITÀ PER I QUALI SONO TRATTATI?	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?	La Piattaforma permette al Segnalante di procedere all'aggiornamento, integrazione o rettifica dei dati originariamente trasmessi con la segnalazione
È STATA CORRETTAMENTE INDIVIDUATA LA BASE GIURIDICA LEGITTIMANTE IL TRATTAMENTO?	La base legittimante il trattamento dei dati personali contenuti nella segnalazione è stata correttamente individuata nella

	necessità di adempiere un obbligo legale al quale è soggetta la Società, in qualità di Titolare del Trattamento
È PREVISTA LA RICHIESTA DI CONSENSO DEL SOGGETTO INTERESSATO/SEGNALANTE?	La Procedura Whistleblowing adottata dalla Società, conformemente al dettato normativo, prevede che venga raccolto il consenso del Segnalante nei seguenti casi: (i) registrazione della segnalazione resa oralmente su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale, (ii) rivelazione della identità del Segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, (iii) rivelazione della identità del Segnalante nel procedimento disciplinare, laddove il disvelamento dell'identità sia indispensabile per la difesa del soggetto a cui viene contestato l'addebito disciplinare, (iv) rivelazione della identità del Segnalante nei procedimenti instaurati in seguito a segnalazioni interne o esterne, laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta.
✓ I principi di necessità e proporzionalità risultano correttamente rispettati; sul punto non si rilevano inadeguatezze del sistema adottato dalla Società.	

11. ANALISI DEI RISCHI PER I DIRITTI E LE LIBERTA' FONDAMENTALI DEGLI INTERESSATI

L'analisi dei rischi richiede la corretta identificazione delle potenziali minacce per i dati personali sottoposti a trattamento nel processo di Whistleblowing.

Le principali minacce sono quelle che riguardano le fondamentali caratteristiche di Riservatezza, Integrità e Disponibilità.

OGGETTO DELLA MINACCIA	TIPOLOGIA	EFFETTI
Riservatezza	Accesso illegittimo	Divulgazione o accesso non autorizzati
Integrità	Modifica indesiderata	Modifica
Disponibilità	Perdita anche momentanea dei dati	Distruzione o perdita

La valutazione del rischio insito nel trattamento viene effettuata attraverso la ponderazione tra la PROBABILITÀ di accadimento della minaccia e l'IMPATTO della stessa sui diritti e le libertà fondamentali dei soggetti interessati.

Rispetto al parametro della Probabilità, in una scala di valori "ALTA-MEDIA-BASSA", nell'estensione della presente valutazione di impatto si è tenuto conto, in primo luogo, del dato storico relativo al limitatissimo numero di segnalazioni whistleblowing ricevute dagli enti già sottoposti all'obbligo normativo di adottare canali interni di segnalazione, prima

dell'entrata in vigore della nuova normativa[1]. A fronte di tale dato storico, nella presente valutazione è stato assegnato alla probabilità di accadimento un valore "medio" in ragione delle modifiche normative introdotte con il D. Lgs 24/2023, con particolare riferimento all'ampliamento delle categorie di violazioni astrattamente segnalabili e alla capillarità dell'attività di formazione e informazione richiesta.

Riguardo al parametro dell'Impatto, invece, si è valutato che le conseguenze derivanti dalla perdita di riservatezza, integrità e disponibilità dei dati personali oggetto di segnalazione si attestino su un livello "alto", potendo i soggetti interessati, con particolare riferimento al Segnalante, subire conseguenze significative, che potrebbero essere superate con gravi difficoltà (es: perdita del posto di lavoro, citazione in giudizio, conseguenze negative rispetto allo stato di salute, ecc.).

A. Perdita di Riservatezza

FONTI DI RISCHIO	ESEMPI MINACCE	PROBABILITÀ DELLA MINACCIA	IMPATTO
INTERCETTAZIONE UMANA O TECNOLOGICA DEI DATI	divulgazione, intenzionale o non intenzionale di informazioni, uso di dispositivi di ascolto per intercettare o registrare le informazioni, acquisizione di dati trasmessi attraverso una rete Wi-Fi, infezioni da malware, ecc.	**MEDIA**	**ALTO**
USO ANOMALO DI SOFTWARE/HARDWARE	utilizzo di USB flash drives o memorie esterne non idonei alla sensibilità delle informazioni, scansioni di contenuti, riferimenti incrociati illeciti, abuso di privilegi sui dati, cancellazione delle tracce di utilizzo, ecc.	**MEDIA**	**ALTO**
PERDITA	furto di documenti, furto di *device*, recupero dati da documenti eliminati in maniera non idonea, contratti di manutenzione inidonei, infezioni da malware, modifica dei soggetti autorizzati al trattamento, ecc.	**MEDIA**	**ALTO**

FONTI DI RISCHIO	MISURE DI SICUREZZA ADOTTATE	STATO ADEGUATEZZA MISURE ADOTTATE	RISCHIO RESIDUO
INTERCETTAZIONE UMANA O TECNOLOGICA DEI DATI	**Controllo degli accessi logici** Possibilità di accesso al sistema mediante **credenziali di**		

[1] Si vedano i report whistleblowing 2020, 2021 e 2022, pubblicati sul sito www.transparency.it

	autenticazione assegnate personalmente **Misure** di **sicurezza dei canali informatici** Utilizzo di **protocolli crittografici** **Registrazione dei log** delle attività del **Segnalante disabilitata** (i log sono privi delle informazioni relative a indirizzi IP e User Agent) **Salvataggio** dei dati su **server esterni** (cloud) a quello aziendale **Gestione delle vulnerabilità tecniche e monitoraggio della sicurezza dell'infrastruttura IT** utilizzata per elaborare e trasferire i dati **Manutenzione** periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza	ADEGUATO	**BASSO**
USO ANOMALO DI SOFTWARE/HARDWARE	**Controllo degli accessi logici** **Formazione specifica** in materia di Whistleblowing e di Data Protection ai soggetti autorizzati **Censimento asset** utilizzati **Sicurezza** dell'**Hardware** **Lotta** contro il **Malware** (firewall e antivirus)	ADEGUATO	**BASSO**
PERDITA	**Politica di Data Retention,** implementata dalla piattaforma e riportata all'interno della Procedura Whistleblowing, allineata al dettato normativo **Gestione delle vulnerabilità tecniche e monitoraggio della sicurezza dell'infrastruttura IT** utilizzata per elaborare e trasferire i dati	ADEGUATO	**BASSO**

	Manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza		

B. Perdita di Integrità

FONTI DI RISCHIO	ESEMPI MINACCE	PROBABILITÀ DELLA MINACCIA	IMPATTO
MODIFICA DEI SISTEMI SOFTWARE/HARDWARE	aggiunta di hardware incompatibili con il sistema, rimozioni di componenti essenziali, cancellazione di *files necessary* per il corretto funzionamento dei software, errori nelle attività di aggiornamento del sistema, infezioni da malware, ecc.	**MEDIA**	**ALTO**
SOVRACCARICO	carichi di lavoro eccessivi, assegnazioni di compiti a personale non preparato/non competente	**MEDIA**	**ALTO**

FONTI DI RISCHIO	MISURE DI SICUREZZA ADOTTATE	STATO DI ADEGUATEZZA MISURE ADOTTATE	RISCHIO RESIDUO
MODIFICA DEI SISTEMI SOFTWARE/HARDWARE	**Sistema di back-up remoto giornaliero** **Separazione fisica** della copia dei dati **Gestione delle vulnerabilità tecniche e monitoraggio della sicurezza dell'infrastruttura IT** utilizzata per elaborare e trasferire i dati **Sistema di approvvigionamento energetico continuo** all'infrastruttura IT utilizzata per elaborare i dati (inclusi i sistemi energetici di emergenza) **Manutenzione** periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza	ADEGUATO	**BASSO**
SOVRACCARICO	**Formazione specifica** in materia di Whistleblowing e di Data Protection ai soggetti autorizzati	ADEGUATO	**BASSO**

C. Perdita di Disponibilità

FONTI DI RISCHIO	ESEMPI MINACCE	PROBABILITÀ DELLA MINACCIA	IMPATTO
DANNI AI SISTEMI SOFTWARE/HARDWARE	Allagamenti, incendi, atti vandalici, danni derivanti da malfunzionamento del sistema o della rete, ecc.	**MEDIA**	**ALTO**
USO ANOMALO DI SOFTWARE/HARDWARE	errata archiviazione, errata cancellazione dei dati, ecc.	**MEDIA**	**ALTO**
PERDITA	furto di documenti, furto di *device*, smaltimento non controllato dei device, contratti di manutenzione inidonei, infezioni da malware, modifica dei soggetti autorizzati al trattamento, ecc.	**MEDIA**	**ALTO**
SOVRACCARICO	Dispositivi di memorizzazione pieni, sovraccarico del database, carichi di lavoro eccessivi, assegnazioni di compiti a personale non preparato/non competente	**MEDIA**	**ALTA**

FONTI DI RISCHIO	MISURE DI SICUREZZA ADOTTATE	STATO DI ADEGUATEZZA MISURE ADOTTATE	RISCHIO RESIDUO
DANNI AI SISTEMI SOFTWARE/HARDWARE	**Sistema di back-up remoto giornaliero** **Separazione fisica** della copia dei dati **Gestione delle vulnerabilità tecniche e monitoraggio della sicurezza dell'infrastruttura IT** utilizzata per elaborare e trasferire i dati **Sistema di approvvigionamento energetico continuo** all'infrastruttura IT utilizzata per elaborare i dati (inclusi i sistemi energetici di emergenza) **Manutenzione** periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza	ADEGUATO	**BASSO**

USO ANOMALO DI SOFTWARE/HARDWARE	**Sistema di back-up remoto giornaliero** **Separazione fisica** della copia dei dati **Formazione specifica** in materia di Whistleblowing e di Data Protection ai soggetti autorizzati	ADEGUATO	**BASSO**
PERDITA	**Politica di Data Retention,** implementata dalla piattaforma e riportata all'interno della Procedura Whistleblowing, allineata al dettato normativo **Formazione specifica** in materia di Whistleblowing e di Data Protection ai soggetti autorizzati	ADEGUATO	**BASSO**
SOVRACCARICO	**Sistema di back-up remoto giornaliero** **Separazione fisica** della copia dei dati **Gestione delle vulnerabilità tecniche e monitoraggio della sicurezza dell'infrastruttura IT** utilizzata per elaborare e trasferire i dati **Manutenzione** periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza **Formazione specifica** in materia di Whistleblowing e di Data Protection ai soggetti autorizzati	ADEGUATO	**BASSO**

12. MISURE CHE CONTRIBUISCONO ALL'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

Obbligo di rendere informazioni e comunicazioni chiare e trasparenti – art. 12 ss. GDPR

La Società ha messo a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne. Le suddette informazioni sono esposte e rese facilmente visibili nei luoghi di lavoro, nonché accessibili alle persone che pur non

frequentando i luoghi di lavoro intrattengono un rapporto giuridico con la Società, mediante pubblicazione sul sito aziendale, al seguente link https://www.gabtamagnini.it/whistleblowing.

Il Segnalante, al momento dell'accesso sul Portale WHISTLEBLOWING, riceve una specifica informativa ai sensi dell'art. 13 GDPR sul trattamento dei dati personali.

Esercizio dei diritti da parte degli interessati - artt. 15 ss GDPR

La Società è dotata di un Sistema di Gestione Privacy che prevede una specifica procedura in materia di gestione delle richieste di esercizio dei diritti esercitate dai soggetti interessati.

Rapporti con i Responsabili del Trattamento – art. 28 GDPR

Tutti i soggetti esterni ai quali il Titolare ha delegato attività di trattamento sono stati selezionati in base a criteri di professionalità ed esperienza, nonché, valutando le garanzie offerte in merito alla protezione dei dati personali.

I soggetti esterni sono stati tutti nominati attraverso la sottoscrizione di appositi atti (art. 28 GDPR) che individuano chiaramente i rispettivi ruoli e responsabilità.

Trasferimento di dati al di fuori dell'Unione europea – artt. 44 ss GDPR

Il Titolare ha avuto modo di verificare che i trattamenti svolti nell'ambito del processo di Whistleblowing avvengono nell'ambito dell'Unione Europea e dello Spazio Economico Europeo.

Gli accordi contrattuali siglati con i Responsabili prevedono che qualora i dati oggetto di trattamento dovessero essere trasferiti al di fuori dell'Unione Europea o dello Spazio Economico Europeo, in luoghi ove non siano state espresse valutazioni di adeguatezza del livello di protezione da parte della Commissione Europea, le condizioni di trasferimento dovranno essere preventivamente concordate con la Società.