

Valutazione d'impatto sulla protezione dei dati ai sensi e per gli effetti dell'art. 35 del Regolamento (UE) n. 2016/679 (DPIA – *Data Protection Impact Assessment*) e del sesto comma dell'art.13 d. lgs. 24/2023
in relazione ai trattamenti connessi all'adempimento delle prescrizioni normative dettate in materia di *Whistleblowing*

1. Premesse

Euromec 2 s.r.l. Società Unipersonale, con sede legale in Portogruaro (Ve) - Via Maestri del Lavoro 6, in qualità di Titolare del trattamento, procede alla presente Valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del GDPR in relazione ai trattamenti connessi all'adempimento delle prescrizioni contenute nel d.lgs. n. 24/2023 - e, per le parti non abrogate, nella legge 179/2017 - dettate in materia di segnalazioni di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità degli enti privati, anche alla luce di quanto previsto nella Procedura di gestione delle suddette segnalazioni (cd. *Procedura Whistleblowing* – Allegato 1) adottata dal Titolare e i cui contenuti, qui integralmente richiamati, sono affissi nella bacheca Aziendale sita presso la suddetta sede legale.¹

La valutazione di impatto in presenza dei trattamenti di cui sopra risulta obbligatoria ai sensi e per gli effetti del sesto comma dell'art.13 d. lgs. 24/2023 in quanto trattasi di operazioni su dati ritenute suscettibili di comportare potenziali rischi per i diritti e libertà delle persone fisiche.

Il presente documento sarà aggiornato alla luce di eventuali modifiche normative e/o organizzative.

Indice generale

1a) Descrizione Sistematica del Trattamento; 1b) Finalità del trattamento dei dati; 1c) Oggetto del trattamento – categorie di dati personali; 1d) Base giuridica del trattamento;
2) Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

¹ La “*Procedura Whistleblowing*” per la gestione interna delle segnalazioni - la quale si avvale sia della piattaforma informatica *Glogal Leaks*, installata nella pagina *web* del sito aziendale del Titolare, sia della possibilità di invio delle segnalazioni attraverso comunicazione scritta in busta chiusa, nominativa oppure anonima - contiene l'elenco delle azioni e dei sistemi adottati da Euromec 2 s.r.l. a tutela dei dipendenti e di tutti i soggetti segnalanti fatti illeciti e irregolarità ai sensi dell'art. 3 d.lgs. 24/2023, oltretutto di quelli coinvolti (segnalati) o comunque menzionati (quali, ad esempio, facilitatori, testimoni) ai sensi del medesimo d. lgs.24/2023, nonché l'indicazione delle modalità di effettuazione e gestione di tali segnalazioni, in conformità a quanto stabilito, in particolare, dagli artt. 4 e 5 del medesimo d.lgs. 24/2023.

L'obiettivo perseguito dalla Procedura è quello di descrivere e regolamentare il processo di segnalazione delle violazioni, fornendo al segnalante chiare indicazioni operative circa l'oggetto, i contenuti, i destinatari e le modalità di trasmissione delle segnalazioni, nonché riguardo alle forme di tutela che vengono predisposte dalla Società in conformità alle disposizioni normative.

La Procedura ha altresì lo scopo di disciplinare le modalità di accertamento della validità e fondatezza delle segnalazioni e, conseguentemente, di intraprendere le azioni correttive e disciplinari opportune a tutela della Società.

La Procedura si applica nell'ambito di tutte le attività aziendali della Società e deve essere fedelmente rispettata dai destinatari, nell'osservanza degli obblighi di legge che potrebbero derivare dalla segnalazione: in particolare, in tema di obbligo di denuncia all'Autorità Giudiziaria e in materia di trattamento dei dati personali il quale deve svolgersi nel rispetto della disciplina interna, comunitaria e internazionale vigente.

3) Valutazione dei rischi per i diritti e le libertà degli interessati e misure di sicurezza adottate;
4) Ulteriori Misure previste per affrontare i rischi, incluse le garanzie, misure di sicurezza dei meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati.

*

1a) Descrizione Sistematica del Trattamento

EUROMECC 2 s.r.l., nell'ambito della predetta procedura, ha affidato ad un **soggetto esterno** all'Azienda la **gestione del canale di segnalazione interno**.

Quanto alle segnalazioni tramite la piattaforma *Global Leaks* esse verranno così gestite:

- * il Gestore esterno rilascerà alla persona segnalante, un avviso di avvenuto ricevimento della segnalazione entro sette giorni dalla data di ricezione della segnalazione;
- * il Gestore esterno manterrà le interlocuzioni con la persona segnalante e potrà richiedere a quest'ultima, se necessario, integrazioni;
- * il Gestore esterno darà diligente seguito alle segnalazioni ricevute;
- * il Gestore esterno fornirà riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

Quanto alle segnalazioni che tramite comunicazione scritta in busta chiusa esse dovranno essere indirizzate all'azienda presso la sede legale della stessa in Portogruaro (Ve) - Via Maestri del Lavoro 6, all'attenzione della Responsabile amministrativa apponendo sulla busta la dicitura: **SEGNALAZIONE WHISTLEBLOWING**. Tale missiva in busta chiusa verrà quindi fatta pervenire al Gestore esterno da parte della Responsabile Amministrativa.

- * il Gestore esterno, ove sia nota l'identità del segnalante, rilascerà alla persona segnalante nei recapiti indicati dal medesimo, un avviso di avvenuto ricevimento della segnalazione entro sette giorni dalla data di ricezione della segnalazione;
- * il Gestore esterno, ove sia nota l'identità del segnalante, manterrà le interlocuzioni con la persona segnalante e potrà richiedere a quest'ultima, se necessario, integrazioni;
- * il Gestore esterno darà diligente seguito alle segnalazioni ricevute;
- * il Gestore esterno, ove sia nota l'identità del segnalante, fornirà riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

Tutti i lavoratori subordinati, autonomi, collaboratori nonché liberi professionisti e consulenti, volontari e tirocinanti che prestano la propria attività presso l'Azienda, retribuiti e non retribuiti, azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, potranno effettuare tramite utilizzo della piattaforma informatica *Global Leaks* ovvero mediante comunicazione in busta chiusa, segnalazioni anche in modo anonimo su violazioni di disposizioni normative nazionali quali: illeciti amministrativi, contabili, civili o penali, condotte illecite ai sensi del decreto legislativo 8

giugno 2001 n. 231, illeciti che rientrano negli atti dell'Unione Europea, violazioni dei modelli di organizzazione e atti o omissioni che ledono gli interessi finanziari dell'Unione.

Tutte le segnalazioni saranno gestite nel rispetto della riservatezza e nella protezione dei dati del segnalante, oltreché, dei soggetti coinvolti (segnalati) o comunque menzionati (quali, ad esempio, facilitatori, testimoni) ai sensi del medesimo d. lgs. 24/2023 e pertanto dovranno avvenire in ottemperanza alle prescrizioni della normativa in tema di protezione dei dati personali di cui al Regolamento Europeo 2016/679 (*General Data Protection Regulation* o GDPR), nonché, in quanto e allorché applicabile, di cui al D. lgs. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*), così come, da ultimo, modificato anche dal D. lgs. 10 agosto 2018, n. 101, oltreché dei Provvedimenti (tra cui, da ultimo anche il Provvedimento n. 146/2019 *recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101*), delle Autorizzazioni, delle Linee Guida dell'Autorità Garante, attualmente vigenti, delle Linee Guida A.N.A.C. del 12 luglio 2023 ("*Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne*") e, in ogni caso, di tutta la disciplina integrativa nazionale, internazionale e comunitaria allo stato applicabile in materia

1b) Finalità del trattamento dei dati

I dati personali forniti e resi disponibili tramite la piattaforma informatica o la comunicazione scritta di cui alla nota 1, ai sensi del d.lgs. 24/2023 (c.d. "*Segnalazione Whistleblowing*") e/o contenuti nella documentazione allegata alla stessa segnalazione o in quella che verrà raccolta nel corso del procedimento, saranno trattati per:

- a) Finalità connesse alla gestione e verifica della segnalazione e, dunque per garantire un'adeguata applicazione della *Procedura Whistleblowing* adottata e, comunque, in ogni caso, ai fini di adempimento degli obblighi di legge in materia.
- b) Finalità di tutela legale e, dunque, per far valere o difendere un diritto anche da parte di un terzo in sede stragiudiziale o giudiziale, nonché in sede amministrativa, disciplinare o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa interna e/o dell'Unione Europea, dai regolamenti, e dai contratti collettivi.

Per le previsioni specifiche relative ai trattamenti aventi ad oggetto i dati dei soggetti segnalanti e quelli dei soggetti diversi da questi ultimi si rinvia *in toto* a quanto contenuto nelle informative sul trattamento dei dati personali rese ai sensi e per gli effetti degli artt. 13 e 14 GDPR di cui rispettivamente agli Allegati 3 e 3 *bis*.

1c) Oggetto del trattamento – categorie di dati personali

Per le previsioni specifiche relative ai trattamenti aventi ad oggetto i dati dei soggetti segnalanti e quelli dei soggetti diversi da questi ultimi si rinvia *in toto* a quanto contenuto nelle informative sul trattamento dei dati personali rese ai sensi e per gli effetti degli artt. 13 e 14 GDPR di cui rispettivamente agli Allegati 3 e 3 *bis*.

La segnalazione non dovrà contenere fatti irrilevanti ai fini della stessa, né categorie particolari di dati personali, di cui all'art. 9 del GDPR (di seguito anche "*categorie particolari di dati*"), cioè quelli da cui possono eventualmente desumersi, fra l'altro, l'origine razziale ed etnica, le convinzioni filosofiche e religiose, l'adesione a partiti o sindacati, nonché lo stato di salute, la vita sessuale o l'orientamento sessuale, salvo i casi in cui ciò sia inevitabile e necessario ai fini della segnalazione stessa.

1d) Base giuridica del trattamento: interesse legittimo perseguito dal Titolare del trattamento

Per le previsioni specifiche relative ai trattamenti aventi ad oggetto i dati dei soggetti segnalanti e quelli dei soggetti diversi da questi ultimi si rinvia *in toto* a quanto contenuto nelle informative sul trattamento dei dati personali rese ai sensi e per gli effetti degli artt. 13 e 14 GDPR di cui rispettivamente agli Allegati 3 e 3 *bis*.

2) Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità

La necessità e proporzionalità del trattamento in oggetto in relazione alle finalità di cui al precedente paragrafo 1)c) sono assicurate dall'esistenza di un obbligo di legge cui il Titolare ha dato attuazione attraverso una specifica Procedura che soddisfa i parametri legali anche in relazione alle misure di sicurezza richieste dalla legge in materia di protezione dei dati personali e che verranno più dettagliatamente descritte ai paragrafi 3 e 4.

Si precisa, al riguardo che il Titolare tratta i dati nel rispetto dell'art. 5 del GDPR il quale impone che i dati siano: "a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati («limitazione della conservazione»); f) trattati 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»)".

3) Valutazione dei rischi per i diritti e le libertà degli interessati e misure di sicurezza adottate

Ai fini di valutare l'adeguatezza del livello di sicurezza dei trattamenti in esame sono stati analizzati i rischi specifici di tali trattamenti distinguendo l'ipotesi in cui le segnalazioni vengano effettuate tramite la piattaforma Global Leaks ovvero tramite comunicazione in busta chiusa.

L'Analisi dei Rischi è stata eseguita tenendo conto degli eventi che, sulla scorta di un giudizio prognostico, potrebbero, con più elevato grado di possibilità/probabilità, incidere, nei termini anzidetti, sulla sicurezza dei dati. A tali eventi è stato associato un grado di possibilità/probabilità del relativo rischio (prendendo a parametro una scala ascendente basso/medio/alto), una indicazione dell'eventuale grado di impatto sui dati (basso/medio/alto) e la correlativa contromisura di sicurezza prevista in ottemperanza al progetto del Titolare.

Segnalazioni tramite la piattaforma Global Leaks

Global Leaks è una piattaforma software progettata per consentire la raccolta e gestione di segnalazioni di illeciti o irregolarità, c.d. Whistleblowing, garantendo la protezione delle persone che le effettuano, in conformità al D.Lgs. 24/2023. Global Leaks viene gestita da Centro Paghe S.r.l., Via Brescia 49 – 36040 Torri di Quartesolo (Vicenza), P.IVA 03042680243.

Di seguito si riportano le informazioni relative alle caratteristiche e alle misure di sicurezza adottate della piattaforma così come illustrate nella relativa Relazione tecnica. Esse riguardano:

- Il trattamento dei dati personali;
- l'architettura e sicurezza;
- la gestione delle identità e degli accessi;
- le modalità di invio e ricezione delle segnalazioni;
- le funzionalità di tracciamento e reportistica.

Trattamento dei dati personali

- Le informazioni raccolte da Global Leaks attengono a: dati anagrafici del segnalante (nome, cognome, recapiti); eventuali dati personali del/i segnalato/i; descrizione del fatto che si intende segnalare; eventuali provvedimenti conseguenti alla segnalazione, adottati dal destinatario della segnalazione. In caso di “segnalazione anonima” viene garantito, oltre alla tutela del contenuto della trasmissione, anche l’anonimato delle transazioni tra il segnalante e il canale Whistleblowing, rendendo impossibile per il destinatario e per tutti gli intermediari nella trasmissione avere traccia del mittente. Global Leaks è in grado di fornire adeguate misure tecniche e organizzative al fine di rendere i trattamenti in linea con i requisiti del Regolamento (UE) 2016/679 (GDPR) e di ogni ulteriore atto con forza di legge o regolamentare in materia di protezione dei dati personali
- Conservazione dei dati. I dati relativi alle segnalazioni saranno conservati dalla piattaforma non oltre cinque anni a decorrere dalla data di comunicazione dell’esito finale della procedura di segnalazione. In caso di controversie, i dati potranno essere conservati per un periodo maggiore, coincidente con la durata della controversia stessa.
- Trasferimento dei dati extra UE.
- I dati potranno essere trasferiti all’interno della Unione Europea. I dati non saranno trasferiti fuori dalla Unione Europea. In particolare, le aziende che collaborano con Centro Paghe S.r.l. per la gestione della piattaforma sono le seguenti: Emisfera Soc. Cooperativa, Shellrent, Aruba.
- Architettura e sicurezza
- Sul punto si rinvia a quanto indicato nel sito di Global Leaks www.globaleaks.org
- Gestione delle identità e degli accessi
- Sul punto si rinvia a quanto indicato nel sito di Global Leaks www.globaleaks.org
- Autenticazione a due fattori con TOTP
- Sul punto si rinvia a quanto indicato nel sito di Global Leaks www.globaleaks.org
- Modalità di invio e ricezione delle segnalazioni
- Il segnalante accede alla piattaforma tramite il portale web e compila un modulo guidato per inviare una nuova segnalazione. Può allegare file e inserire informazioni aggiuntive in modo anonimo o nominale. La segnalazione viene crittografata end-to-end con la chiave pubblica RSA del destinatario. Il destinatario (ruolo keeper) riceve una notifica via email di nuova segnalazione. Accedendo al portale può visualizzare la segnalazione decifrata con la sua chiave privata RSA. Può comunicare in modalità riservata con il segnalante tramite messaggi cifrati E2E per richiedere maggiori dettagli. Al termine dell’analisi, può archiviare la segnalazione con il relativo esito.
- Funzionalità di tracciamento e reportistica
- Tutte le operazioni effettuate sulla piattaforma vengono registrate su un database con un audit trail completo.

Conclusioni

Global Leaks garantisce la conformità normativa e il massimo livello di sicurezza per la gestione del processo di segnalazione interno. La sua architettura è flessibile e consente integrazioni con i sistemi aziendali esistenti. La crittografia end-to-end abbinata alla gestione sicura delle identità

digitali assicura la confidenzialità delle informazioni in ogni fase del processo. Si precisa che Global Leaks allo stato, anche in riferimento ai questionari proposti alla data di redazione del presente documento, è il software adottato dall'ANAC.

Atteso quanto sopra esposto di seguito si indicano i **rischi specifici collegati alla Procedura di segnalazione**:

1) Accesso Illegittimo – perdita di riservatezza dei dati

- Impatto sui oggetti interessati: ALTO
- Rischio collegato agli strumenti (piattaforma):
In ragione delle caratteristiche delle misure tecniche e organizzative sopra indicate la probabilità del verificarsi di tale evento risulta BASSA
- Rischio collegato al comportamento degli operatori in caso si segnalazione attraverso la piattaforma: BASSO
La gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.
- Rischio collegato al comportamento degli operatori in relazione alla segnalazione in forma cartacea (busta chiusa): BASSO - si veda al riguardo anche quanto indicato nella tabella sotto riportata
La prima acquisizione della comunicazione è affidata esclusivamente a personale di fiducia (Responsabile amministrativa) debitamente formato e il cui operato è comunque controllato dal Titolare. Le buste vengono immediatamente indirizzate al Gestore esterno (senza mai aprirle) e ove ciò non sia possibile conservate (senza mai aprirle) fino al momento dell'invio in un armadio munito di chiave a disposizione del solo personale in questione.
La presa in carico e la gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.

2) Modifiche indesiderate – Perdita dell'integrità del dato

- Impatto sui oggetti interessati: ALTO
- Rischio collegato agli strumenti (piattaforma):
In ragione delle caratteristiche delle misure tecniche e organizzative sopra indicate la probabilità del verificarsi di tale evento risulta BASSA
- Rischio collegato al comportamento degli operatori in caso si segnalazione attraverso la piattaforma: BASSO
La gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.
- Rischio collegato al comportamento degli operatori in relazione alla segnalazione in forma cartacea (busta chiusa): BASSO - si veda al riguardo anche quanto indicato nella tabella sotto riportata
La prima acquisizione della comunicazione è affidata esclusivamente a personale di fiducia (Responsabile amministrativa) debitamente formato e il cui operato è comunque controllato dal Titolare. Le buste vengono immediatamente indirizzate al Gestore esterno e ove ciò non sia possibile conservate fino al momento dell'invio in un armadio munito di chiave a disposizione del solo personale in questione.

La presa in carico e la gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.

3) Perdita del dato – perdita della disponibilità

- Impatto sui oggetti interessati: ALTO
- Rischio collegato agli strumenti (piattaforma):
In ragione delle caratteristiche delle misure tecniche e organizzative sopra indicate la probabilità del verificarsi di tale evento risulta BASSA
- Rischio collegato al comportamento degli operatori in caso si segnalazione attraverso la piattaforma: BASSO - si veda al riguardo anche quanto indicato nella tabella sotto riportata
La gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.
- Rischio collegato al comportamento degli operatori in relazione alla segnalazione in forma cartacea (busta chiusa): BASSO
La prima acquisizione della comunicazione è affidata esclusivamente a personale di fiducia (Responsabile amministrativa) debitamente formato e il cui operato è comunque controllato dal Titolare. Le buste vengono immediatamente indirizzate al Gestore esterno e ove ciò non sia possibile conservate fino al momento dell'invio in un armadio munito di chiave a disposizione del solo personale in questione.
La presa in carico e la gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.

4) Comportamenti sleali o fraudolenti

- Impatto sui oggetti interessati: ALTO
- Rischio collegato al comportamento degli operatori in caso si segnalazione attraverso la piattaforma: BASSO
La gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.
- Rischio collegato al comportamento degli operatori in relazione alla segnalazione in forma cartacea (busta chiusa): BASSO - si veda al riguardo anche quanto indicato nella tabella sotto riportata
La prima acquisizione della comunicazione è affidata esclusivamente a personale di fiducia (Responsabile amministrativa) debitamente formato e il cui operato è comunque controllato dal Titolare. Le buste vengono immediatamente indirizzate al Gestore esterno e ove ciò non sia possibile conservate fino al momento dell'invio in un armadio munito di chiave a disposizione del solo personale in questione.
La presa in carico e la gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.

5) Carenza di consapevolezza, disattenzione o incuria

- Impatto sui oggetti interessati: ALTO

- Rischio collegato al comportamento degli operatori in caso di segnalazione attraverso la piattaforma: BASSO

La gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.

- Rischio collegato al comportamento degli operatori in relazione alla segnalazione in forma cartacea (busta chiusa): BASSO - si veda al riguardo anche quanto indicato nella tabella sotto riportata

La prima acquisizione della comunicazione è affidata esclusivamente a personale di fiducia (Responsabile amministrativa) debitamente formato e il cui operato è comunque controllato dal Titolare. Le buste vengono immediatamente indirizzate al Gestore esterno e ove ciò non sia possibile conservate fino al momento dell'invio in un armadio munito di chiave a disposizione del solo personale in questione.

La presa in carico e la gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.

6) Errore materiale

- Impatto sui oggetti interessati: ALTO
- Rischio collegato al comportamento degli operatori in caso di segnalazione attraverso la piattaforma: BASSO

La gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*.

- Rischio collegato al comportamento degli operatori in relazione alla segnalazione in forma cartacea (busta chiusa): BASSO – si veda al riguardo anche quanto indicato nella tabella sotto riportata

La prima acquisizione della comunicazione è affidata esclusivamente a personale di fiducia (Responsabile amministrativa) debitamente formato e il cui operato è comunque controllato dal Titolare. Le buste vengono immediatamente indirizzate al Gestore esterno e ove ciò non sia possibile conservate fino al momento dell'invio in un armadio munito di chiave a disposizione del solo personale in questione.

La presa in carico e la gestione della segnalazione è affidata a soggetto esterno che possiede i requisiti professionali ed organizzativi richiesti per la nomina a Responsabile *ex art. 28 GDPR*

Quanto specificamente ai rischi collegati alla dotazione tecnico-logistica delle strutture in relazione alle segnalazioni inoltrate a mezzo busta chiusa si precisa inoltre che:

Evento	Grado di rischio	Impatto sulla sicurezza dei dati	Misure adottate
Accesso non autorizzato dall'esterno ai locali ove sono presenti i dati	Basso	ALTO	L'armadio in cui sono conservate le buste prima dell'invio al Gestore esterno si trova in un locale chiuso all'esterno con porta munita di chiave in possesso del solo personale autorizzato; l'accesso dalle finestre non è permesso dall'esterno.

Accesso non autorizzato dall'interno alle strutture ove sono collocati i dati	Basso	ALTO	L'armadio in cui sono conservate le buste prima dell'invio al Gestore esterno si trova in un locale chiuso all'esterno con porta munita di chiave in possesso del solo personale autorizzato.
Accesso/sottrazione non autorizzato ai supporti contenenti i dati	Basso	ALTO	L'armadio in cui sono conservate le buste prima dell'invio al Gestore esterno si trova in un locale chiuso all'esterno con porta munita di chiave in possesso del solo personale autorizzato; l'accesso dalle finestre non è permesso dall'esterno.
Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	Basso	ALTO	Vige il divieto di fumare all'interno dei locali ove sono custoditi i dati. Le condutture dell'acquedotto sono conservate in adeguato stato di manutenzione grazie a periodici interventi di tecnici specializzati. Sistema antincendio a norma, manutenzione costante.
Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc)	Basso	ALTO	Gli impianti sono a norma. Viene eseguita una manutenzione costante (vedi sopra). Presenza gruppo di continuità.
Errori umani nella gestione della sicurezza fisica	Basso	ALTO	Idoneo programma di formazione professionale del personale autorizzato e dei Responsabili mediante l'intervento di consulenti specializzati Responsabili dell'adozione misure: Titolare/Responsabili del trattamento

4) Ulteriori specificazioni in relazione alle misure previste per affrontare i rischi, incluse le garanzie, misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati

Il trattamento dei dati personali degli Interessati verrà effettuato con il supporto di mezzi informatici, telematici, e manuali, secondo le modalità previste nella *Procedura Whistleblowing*.

I dati personali verranno trattati e conservati nel pieno rispetto dei principi di necessità, minimizzazione dei dati e limitazione del periodo di conservazione. Il trattamento dei dati personali verrà effettuato in modo da garantire un'adeguata sicurezza e riservatezza in virtù dell'adozione di misure tecniche ed organizzative di carattere fisico, logico e organizzativo adeguate al livello di rischio dei trattamenti volte, tra l'altro, ad impedire la divulgazione, la perdita, l'accesso e l'utilizzo non autorizzato. l'alterazione o la distruzione dei dati personali.

I dati verranno conservati negli archivi fisici ed elettronici del Titolare e del Gestore esterno del canale di segnalazione, quale Responsabile del trattamento ex art. 28 GDPR (v. sul punto anche paragrafo 7) per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, comunque per il periodo previsto dalla legge.

In particolare il Titolare e il Gestore delle segnalazioni conserveranno i dati personali di cui alla segnalazione e la relativa documentazione per il tempo necessario al trattamento della segnalazione in tutte le sue fasi, all'adozione dei provvedimenti conseguenti nonché all'adempimento degli obblighi di legge connessi e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della Procedura di segnalazione, salvo non possano farsi valere termini di conservazione legali maggiori e fatto comunque salvo, in ogni caso, l'eventuale legittimo interesse alla conservazione dei dati necessari per finalità di tutela legale (ad es. a fini di prova dell'adempimento da parte del Titolare delle richieste formulate dall'Interessato nell'ambito dell'esercizio dei propri diritti – sul punto v. il paragrafo 10) nonché il caso in cui la loro ulteriore conservazione sia necessaria per assolvere ad obblighi di legge o per adempiere ad ordini impartiti da Pubbliche Autorità e/o Organismi di Vigilanza ovvero per l'accertamento, l'esercizio o la difesa dei diritti del Titolare o di terzi. Trascorsi i periodi di conservazione sopra indicati, i dati verranno distrutti o resi anonimi in maniera irreversibile.

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione accidentalmente forniti dal segnalante, saranno immediatamente cancellati.

I criteri utilizzati per determinare il periodo di conservazione dei dati sono pertanto:

- a. perseguimento delle finalità relative al trattamento;
- b. tempo di conservazione richiesto per legge;
- c. termine massimo consentito dalla normativa vigente a tutela dei diritti e/o interessi del Titolare.

Con riguardo alle specifiche prescrizioni relative a:

a) Destinatari dei dati personali (soggetti o categorie di soggetti ai quali possono essere comunicati i dati personali o che possono venirne a conoscenza e trattarli in qualità di responsabili o autorizzati al trattamento);

b) Trasferimento dei dati extra UE e processi decisionali automatizzati;

c) Diritti (ulteriori) dell'interessato si rinvia *in toto* a quanto contenuto nelle informative sul trattamento dei dati personali rese ai sensi e per gli effetti degli artt. 13 e 14 GDPR di cui rispettivamente agli Allegati 3 e 3 *bis*.

Alla luce di quanto esposto, le finalità, le modalità e il complesso delle misure di sicurezza e delle garanzie previste a tutela dei dati personali oggetto dei trattamenti che derivano dall'ottemperanza agli obblighi previsti dalla citata normativa in materia di Whistleblowing sopra descritti sono in grado di assicurare la *compliance* al GDPR e, in generale, alla disciplina dettata a protezione dei dati personali applicabile alle operazioni sui dati qui esaminate. In particolare, il sistema di gestione degli specifici rischi ad essi connessi appare idoneo a garantire un adeguato livello di sicurezza e riservatezza dei dati unitamente al rispetto dei diritti e delle libertà dei soggetti interessati.

Allegati:

- 1) Procedura *Whistleblowing* adottata dal Titolare;
- 2) Relazione tecnica piattaforma Global Leaks;
- 3) Informativa sul trattamento dei dati personali resa ai sensi e per gli effetti dell'art. 13-del Regolamento (UE) 2016/679 (*General Data Protection Regulation* o GDPR) per i soggetti che segnalano illeciti a norma del d.lgs. n. 24/2023 (Whistleblower);
- 3 *bis*) Informativa sul trattamento dei dati personali resa ai sensi e per gli effetti dell'art. 14 del Regolamento (UE) 2016/679 (*General Data Protection Regulation* o GDPR) per i soggetti diversi dal segnalante illeciti (Whistleblower) a norma del d.lgs. n. 24/2023;
- 4) Nomina del Gestore esterno delle segnalazioni a Responsabile esterno *ex art.* 28 GDPR.

Portogruaro (VE),

EUROMEC 2 S.R.L.

.....