SILGA
Beyond surfaces

SILGA
Connect technology

SILGA S.p.A.
Procedura di segnalazione Whistleblowing d.lgs. 24/2023

Data Privacy Impact Assessment (DPIA)

SILGA
Industries

Silga S.p.A.
Via C.Marx 54 - I-60022 Castelfidardo AN
silga@isilga.com - silga@pec.silga.com
+39 071 723971

P.Iva e C.F. 00092270420
Codice Identificazione IT 00092270420
Iscritta al n. AN 61210 R.E.A.
Iscritta al n. 00092270420 R.I. MARCHE

Soggetta all'attività di direzione e coordinamento di Zitti Holding Srl

silgaindustries.com
silgagalvanica.com
silgaelectronics.com

ELENCO DELLE REVISIONI

REV.	DATA	NATURA DELLE MODIFICHE	APPROVAZIONE
01	17 Luglio 2023	Prima Emissione	Titolare del trattamento

Premessa

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), la DPIA, Valutazione d'impatto del trattamento del dato sulla protezione dei dati personali, è necessaria qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ciò considerata la natura, il contesto e le finalità del trattamento.

Il GDPR introduce dunque una valutazione di stampo preliminare, che consente al Titolare del trattamento di prendere visione del rischio prima ancora di procedere al trattamento e di attivarsi perché tale rischio possa essere, se non annullato, quantomeno fortemente ridotto.

Gli elementi fondamentali della DPIA risultano pertanto:

- i diritti e le libertà fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR che devono essere rispettati e non possono essere soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi;
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio.

La Metodologia di analisi dei rischi adottata nella conduzione delle attività di Data Privacy Impact Assessment è la metodologia di analisi CNIL del Garante Francese.

Come previsto dal d.lgs. 24/2023, la società Silga S.p.A. S.r.l. ha comunicato alle organizzazioni sindacali più rappresentative, l'attivazione del canale di segnalazione.

Il Titolare, ha ritenuto non necessaria la richiesta di un parere preventivo alle parti interessate, viste le garanzie di sicurezza nel trattamento dei dati e di protezione della riservatezza di tutti i soggetti coinvolti, offerte dal soggetto fornitore della piattaforma e dai Responsabili delle segnalazioni.

2. Contesto

2.1. Panoramica del trattamento

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

La gestione delle segnalazioni viene effettuata attraverso canale interno, tramite piattaforma "IntegrityLog" gestita dalla società Euronext Corporate Services Sweden AB, con sede in Hollandargaatan 17 B, 111 60 Stockhol, di cui vengono riportate le principali caratteristiche.

ARCHITETTURA DI SISTEMA	IntegrityLog è ospitata in AWS ed è distribuito su diverse zone di disponibilità per garantire i requisiti di alta disponibilità non funzionale. L'infrastruttura è fornita utilizzando Terraform Infrastructure as Code (IaC) ed è soggetta al controllo di versione. L'utilizzo dell'approccio IaC consente la standardizzazione, riduce il rischio di configurazione errata e migliora la sicurezza generale. L'infrastruttura è stata progettata per reagire ai picchi di domanda e fornire automaticamente nuova potenza di elaborazione attraverso lo scaling orizzontale, senza alcun impatto di funzionamento del prodotto.
SOFTWARE IMPIEGATO	IntegrityLog è una soluzione SaaS (Software as a Service), interamente ospitata nel cloud Amazon Web Services (AWS). Il prodotto è strutturato attorno a servizi interni che sono autoconsistenti in diversi contenitori. Sfruttando la moderna tecnologia di gestione dei container (Kubernetes) è possibile ottenere, grazie alla progettazione, un meccanismo di fail-sail per i componenti principali. IntegrityLog è in grado di bilanciare il carico su più zone di disponibilità (meccanismo di ridondanza di AWS) garantendo un'elevata disponibilità con tempi di recupero in caso di guasto
GESTIONE IDENTITA' E ACCESSI	Il prodotto è stato progettato per sfruttare diversi servizi AWS in modo

	nativo, e quelli utilizzati per la gestione di autenticazione e autorizzazione sono Cognito e Key Management Service (KMS). Amazon Cognito facilita l'autenticazione e l'autorizzazione degli utenti delle applicazioni ed è strettamente integrato con l'architettura del prodotto. Cognito è configurato per utilizzare l'autenticazione a due fattori (token SMS) che aumenta la sicurezza nell'accesso all'applicazione. Amazon KMS fornisce la capacità di di gestire le chiavi crittografiche, ed è il luogo in cui viene memorizzata ogni Master Key del cliente. L'accesso al KMS è gestito all'interno del contesto di sicurezza di ogni tenant, significa che è impossibile per qualsiasi tipo di utente accedere a chiavi per le quali non è stato specificamente concesso l'accesso.
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.

2.2 Responsabilità connesse al trattamento

Ruolo	Nominativo
Titolare del trattamento	SILGA S.p.A., P.I. 00092270420, con sede legale in Castelfidardo (AN), Zona Ind.le Acquaviva

	alla Via Carlo Marx n. 54
Responsabile del trattamento	Euronext Corporate Services Sweden AB, con sede in Hollandargaatan 17 B, 111 60 Stockholm
Sub Responsabile	Amazon Web Services EMEA SARL ("AWS"). Sede della società: Lussemburgo. Elaborazione in Francia, Irlanda, Lussemburgo. COMPLYLOG ha configurato l'impegno di AWS in modo consapevole per indirizzare l'elaborazione verso aziende all'interno dell'UE/SEE. AWS si avvale dei seguenti sub elaboratori con funzione di infrastruttura e archiviazione digitale: Amazon Data Services Ireland Limited. Sede dell'azienda: Irlanda. Luogo di elaborazione: Irlanda Supporto: Amazon Development Centre Ireland Limited. Sede dell'azienda: Irlanda. Luogo di elaborazione: Irlanda.
Responsabili delle segnalazioni	La segnalazione attraverso il canale interno deve essere indirizzata al Responsabile della segnalazione che è stato incaricato dalla Società di gestire la procedura di segnalazione come previsto dal D. Lgs. 24/2023. I soggetti Responsabili delle segnalazioni sono stati individuati nelle persone del Dott. Paolo Massinissa e del Dott. Marco Cruciani, quali membri dell'Organismo di Vigilanza. Questi sono stati nominati designati del trattamento, ai sensi dell'art. 29 Regolamento europeo 2016/679 e 2 *quaterdecies* d.lgs. 101/2018.

2.3 Standard applicabili al trattamento

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

Regolamento UE n. 2016/679 (c.d. GDPR)
D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018
Direttiva UE 1937/2019
D.lgs. n. 24/2023

2.4 Dati, processi e risorse di supporto

Al momento dell'invio della segnalazione (sia tramite piattaforma che tramite registrazione vocale o incontro con il soggetto Responsabile della segnalazione), sono registrate le informazioni fornite dal segnalante. Tali informazioni possono includere:
a) informazioni di contatto (ad esempio, nome, indirizzo, indirizzo e-mail e numero di telefono) dell'individuo che ha presentato la segnalazione e dell'individuo o degli individui a cui si riferisce il reclamo e
b) dettagli dell'illecito, nonché
c) qualsiasi altro dato personale relativo agli individui menzionati nella segnalazione che possa includere dati personali particolari e giudiziari.
Nel caso in cui la segnalazione porti a un'indagine, verranno aggiunte ulteriori informazioni necessarie per indagare sul sospetto illecito. Queste includono principalmente il nome del sospettato, la posizione, i dettagli dell'illecito e le circostanze che sono alla base della segnalazione. Si raccoglieranno inoltre informazioni dalle fonti ritenute necessarie per indagare sull'illecito sospetto.

2.5 Ciclo di vita del trattamento dei dati (descrizione funzionale)

La piattaforma è stata scelta in base ai requisiti indicati dall'art. 13 D. Lgs. 24/2023 e dalle Linee Guida ANAC 2021 e 2023.

Il sistema software preposto alla gestione delle segnalazioni è fruito in modalità SaaS (vale a dire, come "Software as a Service").
Il ciclo di vita dei dati prevede:

1. Attivazione e configurazione della piattaforma.
2. Utilizzo della piattaforma – invio delle segnalazioni da parte dei segnalanti tramite collegamento QR Corde inserito all'interno della procedura e accesso alle stesse da parte dei soggetti autorizzati.
3. Nella piattaforma, la segnalazione viene effettuata compilando il relativo form.
4. Al momento dell'invio della segnalazione, il segnalante riceve un codice numerico univoco che deve conservare per poter accedere nuovamente alla segnalazione, verificare la risposta e dialogare rispondendo a richieste di chiarimenti o approfondimenti.
5. Il codice numerico, se oggetto di smarrimento non può essere rigenerato.

6. La segnalazione può essere effettuata da qualsiasi dispositivo digitale (pc, tablet, smartphone).
7. La tutela della riservatezza è garantita in ogni fase del processo di segnalazione. L'inserimento dei dati personali, quali nome, cognome, numero di telefono, e-mail e posizione lavorativa, non è obbligatorio e può avvenire anche in fase successiva.
8. Nel caso in cui la segnalazione sia anonima – come visto sopra – sarà trattata al pari di una segnalazione ordinaria, solo se il soggetto Responsabile della segnalazione, avrà valutato la suddetta sufficientemente circostanziata.
9. Nessun soggetto all'interno di società Silga S.p.A. (dipendenti, collaboratori, consulenti, ecc.) tratterà i dati personali relativi al segnalante o ad altri soggetti coinvolti dalla segnalazione.
10. Cancellazione dei dati entro 5 ani dal termine dell'istruttoria da parte del soggetto Responsabile della segnalazione.
11. Dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.

2.6. Risorse a supporto dei dati

La piattaforma del fornitore è fruita in modalità Saas.

3. Principi Fondamentali

Gli scopi del trattamento sono specifici, espliciti e legittimi?	Il trattamento è finalizzato esclusivamente alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing. Le finalità sono espresse chiaramente dall'informativa fornita agli interessati
Quali sono le basi giuridiche che rendono lecito il trattamento?	Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui è tenuto il titolare ex d.lgs. 24/2023 il quale prevede l'obbligo di predisporre una procedura di whistleblowing (Art. 6.1. lett. c) GDPR).

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D.lgs. n. 24/2023. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (art. 5.1. lett. c) GDPR).
I dati sono esatti e aggiornati?	Il trattamento dei dati personali relativi alle segnalazioni sono costantemente aggiornati in quanto i soggetti incaricati di ricevere e gestire le segnalazioni ne verificano preliminarmente la corrispondenza a verità.
Qual è il periodo di conservazione dei dati?	Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 14/2023.

3.1. 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. 13-14 GDPR. L'informativa viene resa disponibile secondo le seguenti modalità: 1. Processo comunicazione aziendale sull'esistenza del canale di segnalazione interno (canale informatico). 2. Pubblicazione sul sito aziendale del link per l'accesso alla piattaforma e della procedura.

Ove applicabile: come si ottiene il consenso degli interessati?	Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (Art. 6.1. lett. c) del GDPR).
Come fanno gli interessati a esercitare i loro diritti previsti dagli artt. 15 ss. GDPR?	Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso il contatto con i soggetti gestori delle segnalazioni tramite la piattaforma nei limiti di cui all'articolo 2-undecies del Codice Privacy
Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del trattamento ai sensi dell'art. 28 GDPR, attraverso contratti o altri atti giuridici con indicazione degli obblighi e delle istruzioni per il trattamento dei dati.
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.

4. Misure esistenti

Crittografia	Ogni informazione viene protetta in transito da Crittografia/tunneling (VPN = Virtual Private Network). Amazon KMS fornisce la capacità di gestire le chiavi crittografiche, ed è il luogo in cui viene memorizzata ogni Master Key del cliente. L'accesso al KMS è gestito all'interno del contesto di sicurezza di ogni tenant, Ciò significa che è impossibile per qualsiasi tipo di utente accedere a chiavi per le quali non è stato specificamente concesso l'accesso.

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. Sono stati impostati: • Procedure per la password (compresi caratteri speciali, lunghezza minima, cambio della password); • Blocco automatico (ad es. password o timeout); • Crittografia dei supporti di dati.
Controllo degli accessi ai dati presso i Data center	Sono stati impostati: • Diritti di accesso differenziati (profili, ruoli, transazioni e oggetti); • Segnalazioni; • Accesso; • Cambio; • Cancellazione.
Controllo dell'accesso ai Data center e Sicurezza dell' Hardware	• Sistema di controllo degli accessi • Lettore ID, carta magnetica, chip card • (Rilascio di) chiavi • Chiusura delle porte (apriporta elettrici, ecc.) • Personale di sicurezza, inservienti • Strutture di sorveglianza • Sistema di allarme, monitor video/CCTV
Tracciabilità	Nel caso di accesso al canale interno di segnalazione tramite rete dati interna mediato da dispositivi firewall o proxy, viene garantita la non tracciabilità, sia sulla piattaforma informatica che negli apparati di rete eventualmente coinvolti nella trasmissione o monitoraggio delle comunicazioni, del segnalante nel momento in cui viene stabilita la connessione a tali canali

Controllo della divulgazione	• Crittografia/tunneling (VPN = Virtual Private Network) • Firma elettronica • Registrazione
Controllo dell'Input	Sistemi di registrazione e rendicontazione
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. • Procedure di backup • Mirroring di dischi rigidi, ad es. tecnologia RAID • Gruppo di continuità (UPS) • Archiviazione remota • Sistemi antivirus/firewall; • Piano di ripristino di emergenza. IntergityLog gestisce 2 tipi di dati: informazioni e informazioni basate su file. Per archiviare queste informazioni, vengono utilizzati i servizi nativi di AWS come Dynamo DB per archiviare tutti i dati dell'applicazione e i bucket S3 per archiviare tutti i file. Tutti i dati sono crittografati in transito (crittografia end-to-end) e a riposo (in Dynamo e S3), per garantire la massima riservatezza. Infrastruttura e archiviazione digitale: - Amazon Data Services Ireland Limited. Sede dell'azienda: Irlanda. Luogo di elaborazione: Irlanda Supporto: - Amazon Development Centre Ireland Limited. Sede dell'azienda: Irlanda. Luogo di elaborazione: Irlanda.
Gestione delle vulnerabilità tecniche	L'applicativo è monitorato 24 ore su 24, 7 giorni su 7, dal centro operativo specializzato di Euronext, che segue da vicino molteplici metriche in tempo quasi reale. Queste metriche coprono tutti gli aspetti rilevanti

	dell'infrastruttura, come il provisioning della capacità, lo stato di salute di database e dei cluster di calcolo, ma anche gli aspetti applicativi, come lo stato di salute dei servizi e la gestione degli errori. La centralizzazione di tutti i registri delle applicazioni consente di effettuare indagini forensi e garantisce la verificabilità di ciò che accade all'interno del sistema.
Backup	Tutti i dati memorizzati all'interno dell'applicativo hanno politiche ben definite per garantire la conformità con la normativa sulla conservazione dei dati. I backup dei dati vengono eseguiti in modo incrementale attraverso i meccanismi interni di AWS e garantiscono un Recovery Time Objective (ultime informazioni impegnate).
Manutenzione	L'utilizzo di container per ospitare i prodotti garantisce un controllo granulare sui diversi servizi. Il fornitore della piattaforma è in grado di eseguire un rollout graduale di una nuova versione del prodotto aggiornando in modo incrementale i servizi, oppure con un approccio "big bang", se necessario. Qualsiasi aggiornamento del software viene eseguito nell'ambito delle finestre di manutenzione definite e non avrà alcun impatto sulla disponibilità del servizio.
Sicurezza canali informatici	L'applicativo è monitorato dal sistema di Security Operation Center (SOC) che controlla attivamente i perimetri di sicurezza del prodotto. Questo comporta un approccio esterno convalidando continuamente gli endpoint pubblici e mediante il monitoraggio degli eventi di sicurezza del prodotto. Sono stati predisposti meccanismi per monitorare e

	rispondere a qualsiasi vettore di attacco DDOS, e sono stati implementati forti controlli tramite AWS Shield, per garantire un impatto minimo su tutti gli aspetti del prodotto.
Gestire gli incidenti di sicurezza e le violazioni dei dati personali Lotta contro il malware	Il prodotto è conforme con le normative GDPR in materia. Il titolare si è dotato di un team di risposta in caso di Data Breach e di procedure adeguante alla normativa di settore. Tutti i computer del personale di COMPLYLOG EURONEXT GROUP e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online. Il personale della società Silga S.p.A. esegue formazione in materia di protezione dei dati personali e di cybersecurity.
Politica di tutela della privacy	La società adotta un Modello Organizzativo sulla protezione dei dati personali.
Gestione dei rischi	L'analisi dei rischi viene condotta secondo metodologia Iso 31000 e linee guida ENISA
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 Amministratori di Sistema incaricati dal Titolare del trattamento (a seconda di quanto definito nell'organigramma privacy aziendale).

5. Rischi

5.1 Metodologia

In riferimento alla procedura "Valutazione del Rischio", come indicato dal considerando 76, del GDPR l'azienda si è dotata di un sistema di calcolo del rischio basato su parametri oggettivi, al fine di stabilire se esiste un rischio o un rischio elevato per il trattamento specifico. L'Oggettivazione del rischio pertanto passa attraverso un modello di creazione della Probabilità e della Gravità in grado di rispecchiare il contesto in cui l'organizzazione opera. Sono state identificate griglie oggettive di calcolo delle Probabilità e Gravità con riguardo ai diritti e libertà dell'interessato.

Matrice Ri = P x G					
	Probabilità	1 - Trascurabile	2 – Limitata	3 – Importante	4 – Massima
Gravità	1 - Trascurabile	1	2	3	4
	2 – Limitata	2	4	6	8
	3 – Importante	3	6	9	12
	4 – Massima	4	8	12	16

Gravità	Significato	Descrizione generica degli impatti (diretti e indiretti)
4	Massima	I soggetti interessati possono incontrare conseguenze irreversibili.
3	Importante	I soggetti interessati possono incontrare conseguenze significative, e difficoltà nella loro risoluzione, ma comunque superabili.
2	Limitata	I soggetti interessati possono incontrare inconvenienti superabili.
1	Trascurabile	Gli interessati non saranno coinvolti o potrebbero incontrare alcuni lievi inconvenienti senz'altro superabili.

Probabilità	Significato	Criterio di scelta
4	Massima	Il verificarsi del danno dipende da condizioni direttamente connesse alla situazione; Il verificarsi del danno non provocherebbe alcuna reazione di stupore; Eventi simili sono già accaduti in azienda o in aziende dello stesso tipo
3	Importante	Il verificarsi del danno dipende da condizioni non direttamente connesse alla situazione ma possibili; Il verificarsi del danno provocherebbe reazioni di moderato stupore; Eventi simili sono stati già riscontrati
2	Limitata	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili si sono verificati molto raramente
1	Trascurabile	Il verificarsi del danno è subordinato a un concatenamento di eventi indipendenti tra loro; Il Verificarsi del danno è creduto impossibile dagli addetti; Non è mai accaduto nulla di simile

Valutazione % delle Misure Esistenti

Rating	Descrizione
1-25%	Non adeguate
26-50%	Minime
51-75%	Adeguate

Rating rischio residuo (Rr)

Rischio Alto	6,1-16
Rischio Medio	3,1-6
Rischio Basso	1-3

Elementi per la valutazione:

- Ri è il Rischio Inerente valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione
- Rr è il Rischio Residuo calcolato al netto delle misure di mitigazione del rischio (determinate in via percentuale - % abbattimento)
- L'azienda valuta come Rischio Accettabile (Ra) = 3
- Se il rischio inerente Ri a seguito delle valutazioni oggettive, dovesse risultare superiore ad Ra,
  l'azienda interverrà con mitigazioni opportune tali che ad Rr < Ra

5.2 Analisi dei rischi

5.2.1 Accesso illegittimo – Perdita della riservatezza

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze gravi con conseguenze che possono essere irreversibili. Possono verificarsi: diffusione indesiderata dei propri dati, consultazione dei propri da parte di personale non autorizzato, ricatto economico, problematiche di natura giuslavoristica e contrattuale, sanzioni disciplinari, mobbing, discriminazioni lavorative, demansionamento, ritorsioni.
PROBABILITÀ (P)	La probabilità è molto bassa in quanto solo i soggetti Responsabili delle segnalazioni conoscono l'identità del segnalante e degli altri soggetti coinvolti dalla segnalazione.
FONTI DI RISCHIO	Fonti umane quali i Responsabili delle segnalazioni interne la cui condotta può essere accidentale o intenzionale. Fonti umane esterne (es. fornitori la cui

	condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. attacchi hacker e virus informatici)
MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento
CALCOLO DEL RISCHIO RESIDUO	

G	P	Ri	Mitigazione % abbattimento rischio	Rr
4	2	8	80%	1,6

5.2.2. Modifiche indesiderate – Perdita dell'integrità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: lesione della reputazione, disagio, diffusione indesiderata dei propri dati, consultazione dei propri da parte di personale non autorizzato, sanzioni disciplinari, ricatto economico, problematiche di natura giuslavoristica e contrattuale, mobbing, demansionamento, ritorsioni.
PROBABILITÀ (P)	La probabilità è molto bassa in quanto solo i soggetti Responsabili delle segnalazioni conoscono l'identità del segnalante e degli altri soggetti coinvolti dalla segnalazione.
FONTI DI RISCHIO	Fonti umane quali i Responsabili delle segnalazioni interne la cui condotta può essere accidentale o intenzionale. Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o

	intenzionale, attaccanti e hacker, virus) Fonti non umane (black out, allagamenti, materiali pericolosi).
MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento.
CALCOLO DEL RISCHIO RESIDUO	

G	P	Ri	Mitigazione % abbattimento rischio	Rr
3	2	6	70%	1,8

5.2.3. Perdita del dato – Perdita della disponibilità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze trascurabili o al più limitate, come dover ripresentare la segnalazione.
PROBABILITÀ (P)	La probabilità è molto bassa date le garanzie di sicurezza offerte dalle misure di sicurezza adottate.
FONTI DI RISCHIO	Fonti umane quali i Responsabili delle segnalazioni interne la cui condotta può essere accidentale o intenzionale. Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker, virus) Fonti non umane (es. black out, allagamenti, materiali pericolosi o virus informatici).
MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento.
CALCOLO DEL RISCHIO RESIDUO	

G	P	Ri	Mitigazione % abbattimento	Rr

				rischio	
	2	2	4	70%	1,2

6 Conclusioni

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono "rischi inerenti (Ri)" con impatto sui diritti e libertà degli interessati con stima a valore medio/alto. Nell'ottica di mitigazione di tali rischi, si evince che, con l'implementazione delle misure tecnico/organizzative pianificate ad integrazione di quelle già messe in atto, il valore di rischio residuo rientra nei parametri accettabili uguali o minori rispetto al Rischio accettato (Ra) dall'organizzazione aventi stima a valore basso, valore ritenuto accettabile dall'organizzazione in relazione dai parametri oggettivi considerati.

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

F.to Silga S.p.A. in persona del legale rappresentante p.t.

SILGA Industries
Silga S.p.A.
Presidente e Amministratore Delegato
MONICA ZITTI