Valutazione di impatto
Data Protection Impact Assessment
Gestione delle segnalazioni *whistleblowing*

La presente valutazione di impatto, eseguita ai sensi del Regolamento EU 679/2016 (in seguito, "**GDPR**"), è relativa all'attività di gestione delle segnalazioni ai sensi del decreto legislativo 10 marzo 2023, n. 24 (in seguito, "**d.lgs. n. 24/2023**") svolta da **Giovenale S.r.l.** (in seguito, la "**Società**").

La valutazione di impatto intende fornire il contesto, nonché le informazioni tecniche e di sicurezza adottate per l'acquisizione, il trattamento e l'utilizzo dei dati personali raccolti nell'ambito dell'attività di gestione delle segnalazioni ai sensi del d.lgs. n. 24/2023, in conformità con il GDPR. Si applicano, altresì, le linee-guida del Gruppo Articolo 29 (WP29) concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un Trattamento "possa presentare un rischio elevato" ai sensi del GDPR, adottate il 4 aprile 2017 (versione successivamente emendata e adottata il 4 ottobre 2017).

1. Contesto e finalità 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 un canale adottato dalla Società e implementato da un fornitore esterno, di cui vengono di seguito riportate le principali caratteristiche.

2. Titolare del Trattamento

Il Titolare del trattamento è **Giovenale S.r.l.**, con sede legale in Milano, Corso Giacomo Matteotti, 10 – 20121, C.F. e P.IVA 10895560968.
È possibile contattare gratuitamente il Titolare del Trattamento scrivendo all'indirizzo di posta elettronica privacy.giovenale@colliersglobalinvestors.com, oppure inviando una raccomandata con ricevuta di ritorno presso la sede legale, come sopra individuata.

Il Responsabile della Protezione Dati (DPO) nominato dal Titolare del trattamento è l'avvocato Francesco Conti. È possibile contattare gratuitamente e liberamente il Responsabile della Protezione Dati all'indirizzo e-mail già indicato, oltre che all'indirizzo PEC: francesco.conti@milano.pecavvocati.it.

3. Responsabili del Trattamento

Responsabile del Trattamento è **Testudo S.r.l.**, con sede legale in Milano, via Picco 31, P. IVA IT10520950964, incaricata di fornire la piattaforma per la gestione delle segnalazioni ai sensi del d.lgs. n. 24/2023, denominata "Sibilus" (in seguito, la "**Piattaforma**").

4. Dati personali oggetto del Trattamento e categorie di interessato

La Società tratterà dati identificativi dell'interessato come nome e cognome, dati di contatto, carica o posizione lavorativa, luogo di lavoro, nonché altre informazioni relative all'interessato

incluse nelle segnalazioni o acquisite nel corso dell'istruttoria avviata dal gestore della segnalazione (anche riconducibili alle particolari categorie di dati personali ai sensi degli artt. 9 e 10 del GDPR).

Gli interessati sono i dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto, ovvero fornitori che effettuano una segnalazione o vengono segnalati.

5. Finalità del trattamento

I dati personali potrebbero essere utilizzati per le seguenti finalità:

(i) adempimento agli obblighi di legge a cui è soggetta la Società;
(ii) proteggere il personale della Società, il patrimonio e i beni aziendali;
(iii) prevenire, investigare e perseguire la commissione di reati e condotte disciplinarmente rilevanti;
(iv) accertare, esercitare o difendere un diritto in sede giudiziaria o amministrativa ovvero nell'ambito di procedure di arbitrato o conciliazione.

6. Liceità del trattamento. Basi giuridiche.

La base giuridica del trattamento dei dati personali costituita:

- con riferimento alla lettera (i) del precedente par. 5, dall'adempimento delle disposizioni di legge ai sensi dell'art. 6(1)(c) del GDPR;
- con riferimento alle lettere (ii), (iii) e (iv) del precedente par. 5, dal perseguimento dei legittimi interessi del Titolare ai sensi degli artt. 6(1)(f) e 9(2)(f) del GDPR.

7. Periodo di conservazione.

I dati personali inclusi nelle segnalazioni e nella relativa documentazione saranno conservati per il tempo necessario a dare seguito alle stesse e comunque per non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

La Piattaforma provvede alla cancellazione delle segnalazioni scadute al termine del periodo di conservazione automaticamente e in modalità sicura.

Nel caso in cui, a seguito della segnalazione, la Società avviasse un procedimento disciplinare o promuovesse un procedimento in sede giudiziaria o amministrativa ovvero una procedura di arbitrato o di conciliazione, i dati personali dell'interessato saranno conservati per un tempo pari alla durata del procedimento ovvero al periodo di prescrizione dei diritti per il cui accertamento, esercizio o difesa il trattamento si rende necessario, anche se superiore ai periodi di conservazione indicati sopra.

Testudo S.r.l. provvede alla cancellazione di tutte le segnalazioni della Piattaforma 15 giorni dopo la disattivazione del servizio, comprese quelle coinvolte in contenziosi giudiziari, previa esportazione e trasferimento al titolare delle segnalazioni non ancora scadute.

8. Misure a tutela degli 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:

- processo di comunicazione aziendale sull'esistenza del canale di segnalazione interno (canale informatico);
- pubblicazione sul sito internet della procedura whistleblowing.

Gli interessati possono esercitare i propri diritti, tra i quali quelli di accesso e di portabilità dei dati, di rettifica e di cancellazione (diritto all'oblio), di limitazione e di opposizione, tramite la casella e-mail privacy.giovenale@colliersglobalinvestors.com.

9. Garanzie per i trasferimenti internazionali di dati

I dati non sono trasferiti fuori dall'Unione Europea.

10. Misure di sicurezza esistenti

La gestione delle segnalazioni viene effettuata attraverso la Piattaforma adottata dal Titolare del Trattamento e implementata da un fornitore esterno, Testudo S.r.l., all'uopo nominata responsabile del trattamento ai sensi dell'art. 28 GDPR.
Testudo S.r.l. ha ottenuto le seguenti certificazioni: ISO 27001 – ISO 37001:2021 – ISO 9001.
Si illustrano di seguito le misure di sicurezza esistenti, implementate dal fornitore per garantire la sicurezza dei *servers* e del sito internet che ospita la Piattaforma.

10.1. Risorse di supporto ai dati

La Piattaforma è stata realizzata avvalendosi delle più moderne tecnologie di orchestrazione e containerizzazione: (i) Kubmetes; (ii) Docker.

10.2. Minimizzazione dei dati

Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati, quali la Piattaforma, i log di sistema e i firewall, sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante (ad esempio indirizzi IP, User Agents e altri Metadata). La Piattaforma consente la navigazione tramite Tor Browser per finalità di accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

10.3. Esattezza dei dati

L'aggiornamento dei dati avviene a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata.
Non appena vengono modificati i dati di contatto all'interno della Piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.

10.4. Crittografia

Tutti i dati sono criptati.
Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.

Ogni informazione circa le segnalazioni e i relativi metadati registrata dalla Piattaforma viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni.
Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento.
La Piattaforma è installata su sistema operativo Linux su cui è attiva la *Full Disk Encryption* (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.
Viene utilizzato l'*HyperText Transfer Protocol over Secure Socket Layer* (HTTPS) che fornisce come requisiti chiave un'autenticazione del sito web visitato, protezione della privacy (riservatezza o confidenzialità) e integrità dei dati scambiati tra le parti comunicanti.

10.5. Controllo degli accessi logici

L'accesso alla Piattaforma è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa una policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa un protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

10.6. Tracciabilità

La Piattaforma implementa un sistema di audit log sicuro e *privacy preserving*, atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.

10.7. Archiviazione

La Piattaforma implementa un database *Postgre SQL* acceduto tramite host locale in un *virtual private cloud*.
Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità di sicurezza del database e delle policy di *data retention* e cancellazione sicura.

10.8. Vulnerabilità

Sono effettuati VA / PT mensilmente, per i PT il risultato é disponibile sul sito del fornitore, per le VA viene utilizzato il *tools renovate* che crea delle PR analizzate mensilmente per valutare come procedere agli update delle dipendenze.

10.9. Backup

Sono effettuati automaticamente backup giornalieri rotativi per 14 giorni e test di ripristino in ambiente di *staging*.

10.10. Manutenzione

La manutenzione viene eseguita in modalità a caldo e rotativa.
È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza.

Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale di Testudo S.r.l. attraverso cui svolgere le modifiche al sistema e installare gli aggiornamenti previsti.
Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale di Testudo S.r.l. e/o del relativo fornitore IaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

10.11. Sicurezza dei canali informatici

Tutte le connessioni sono protette tramite protocollo TLS 1.2.
Le connessioni privilegiate dei sistemisti sono mediate tramite connessioni con protocollo SSH.

10.12. Sicurezza dell'hardware

I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24.
I datacenter del fornitore IaaS sono certificati ISO 27001.

10.13. Lotta contro il malware

Tutti i computer del personale della Società e di Testudo S.r.l. eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con Io stato dell'arte in materia di lotta contro il malware.

10.14. Gestione del personale

La Società e Testudo S.r.l. hanno provveduto e provvedono costantemente alla formazione dei soggetti designati/autorizzati al trattamento dei dati personali.
I soggetti designati/autorizzati al trattamento dei dati sono nominati con specifici atti e sono istruiti e formati sul corretto trattamento.

10.15. Restrizioni d'accesso ai dati

L'accesso ai dati del segnalante è effettuabile solo dal gestore della segnalazione stessa tramite la Piattaforma. L'accesso alla segnalazione è limitato alle persone autorizzate come previsto dalla procedura whistleblowing.

10.16. Riduzione della natura identificativa dei dati

I dati vengono criptati con la chiave in possesso della Società.
Il sistema può consentire che l'utente utilizzi una risorsa o un servizio senza rivelare la propria identità (TOR browser).

10.17. Autenticazione e password

Le password non vengono salvate in chiaro sul database, ma subiscono un processo di crittografia tramite *hashing* per prevenire il furto di credenziali.
Al momento del login Testudo S.r.l. confronta la password inserita dall'utente "hashata" con *salt randomico* (salvato sull'utente in fase di impostazione password) con la password criptata salvata sul database. Solo se i due risultati coincidono l'utente riceve il permesso di login.

Testudo S.r.l. non può in ogni caso risalire alla password salvata sul database, trattandosi di password criptata.

11. Analisi dei rischi

A. Violazione della riservatezza, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali	**IMPATTO SUGLI INTERESSATI**	Medio – una perdita della riservatezza potrebbe permettere il tracciamento dell'interessato
	PRINCIPALI MINACCE	Attacchi informatici
	FONTI DI RISCHIO (umane e non)	Procedure non stringenti sulla gestione del dato, disattenzione, ritorsioni, minacce informatiche
	MISURE CHE CONTRIBUISCONO A MITIGARE IL RISCHIO	Tracciabilità, controllo degli accessi fisici, prevenzione delle fonti di rischio, politica di tutela della privacy, vigilanza sulla protezione dei dati, controllo degli accessi logici, sicurezza dei canali informatici, sicurezza dell'hardware, protezione contro fonti di rischio non umane
	GRAVITÀ DEL RISCHIO (impatti potenziali e misure pianificate)	Medio
	PROBABILITÀ DEL RISCHIO – RISCHIO RESIDUO (valutando le misure implementate)	Basso
B. Violazione dell'integrità, in caso di modifica non autorizzata o accidentale dei dati personali	**IMPATTO SUGLI INTERESSATI**	Basso – una perdita dell'integrità non avrebbe conseguenze sui diritti o sulle libertà dell'interessato
	PRINCIPALI MINACCE	Personale operante per conto del Responsabile malintenzionato o disattento, o attacco informatico
	FONTI DI RISCHIO (umane e non)	Procedure non stringenti sulla gestione del dato, disattenzione, ritorsioni, minacce informatiche
	MISURE CHE CONTRIBUISCONO A MITIGARE IL RISCHIO	Tracciabilità, controllo degli accessi fisici, prevenzione delle fonti di rischio, politica di tutela della privacy, gestione del personale, vigilanza sulla protezione dei dati, controllo degli accessi logici, sicurezza dei canali informatici, sicurezza dell'hardware, protezione contro fonti di rischio non umane
	GRAVITÀ DEL RISCHIO (alla luce degli impatti potenziali e delle misure pianificate)	Basso
	PROBABILITÀ DEL RISCHIO – RISCHIO RESIDUO (valutando le misure implementate)	Basso
C. Violazione della disponibilità, in caso di	**IMPATTO SUGLI INTERESSATI**	Basso – una perdita dell'integrità non avrebbe conseguenze sui diritti o sulle libertà dell'interessato
	PRINCIPALI MINACCE	Attacchi informatici, malware

perdita, accesso o distruzione accidentali o non autorizzati di dati personali	**FONTI DI RISCHIO (umane e non)**	Minacce informatiche
	MISURE CHE CONTRIBUISCONO A MITIGARE IL RISCHIO	Tracciabilità, controllo degli accessi fisici, prevenzione delle fonti di rischio, politica di tutela della privacy, integrazione della protezione della privacy nei progetti, gestione del personale, vigilanza sulla protezione dei dati, controllo degli accessi logici, sicurezza dei canali informatici, sicurezza dell'hardware, protezione contro fonti di rischio non umane
	GRAVITÀ DEL RISCHIO (alla luce degli impatti potenziali e delle misure pianificate)	Basso
	PROBABILITÀ DEL RISCHIO - RISCHIO RESIDUO (valutando le misure implementate)	Basso

12. Conclusioni

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono rischi residui con impatto sui diritti e libertà degli interessati con stima a valore **basso**. Il rischio è, sostanzialmente, mitigato dal Titolare tramite le misure di sicurezza attualmente implementate (meglio descritte al precedente par. 10).

Il presente documento sarà eventualmente aggiornato alla luce di modifiche normative e organizzative.

Milano,
Giovenale S.r.l.