Consorzio informatica
Territorio S.p.A.
Via del Commercio, 29
26013 Crema (CR)
Tel: 0373218820
Pec: consorzioit@pec.it
Email: segreteria@consorzioit.net
Cap. Soc. € 2.000.000 i.v.
Cod. Fisc. P.IVA e Reg. Imp. 01321400192
N. iscrizione R.E.A. 161251

Data Privacy Impact Assessment (DPIA)

Whistleblowing - Consorzio IT

ELENCO DELLE REVISIONI

REV.	DATA	NATURA DELLE MODIFICHE	APPROVAZIONE
01	15 luglio 2023	Prima Emissione	Titolare del trattamento

1. Premessa

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), la DPIA corrisponde alla valutazione d'impatto del trattamento del dato sulla protezione dei dati personali, 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.

I principi fondamentali della DPIA risultano pertanto:

- i diritti e le libertà fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR;
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio.

Una DPIA poggia su due pilastri:

1. i principi e i diritti fondamentali, i quali sono "non negoziabili", stabiliti dalla legge e che devono essere rispettati e non possono essere soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi;

2. la gestione dei rischi per la privacy dei soggetti interessati, che determina i controlli tecnici e organizzativi opportuni a tutela dei dati personali.

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 (o altra metodologia definita dal Titolare del trattamento).

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 esterno (piattaforma adottato dalla Società, di cui vengono riportate le principali caratteristiche.

ARCHITETTURA DI SISTEMA	Una macchina virtuale con sistema operativo Ubuntu Linux 16.04.5 LTS, attestata presso il provider SERVERPLAN.
SOFTWARE IMPIEGATO	All'interno del sistema Ubuntu sono configurati i seguenti moduli open source: - un firewall (Iptables) per la protezione di rete - un server di posta (Exim) per la spedizione delle email di servizio - un motore di database (MySql) per conservare i dati di Sestante - un server https (Apache) che smista gli accessi web delle utenze e abilita la crittografia end-to-end È presente inoltre un modulo proprietario (R1Soft) che consente a SERVERPLAN di automatizzare e schedulare i backup della macchina virtuale, come da piano di prevenzione.

	L'applicativo Sestante consta di un software sviluppato in-house con tecnologia Java 8. Il lato front-end utilizza la tecnologia offerta dal framework open-source Vaadin 14. Il lato back-end utilizza i framework open-source Spring Boot, Quartz, EclipseLink.
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	Consorzio It S.p.a.
Responsabile del trattamento	Sage S.r.l.
Sub Responsabile	Master House S.r.l.
Incaricati al trattamento	RPCT e ODV

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

Di seguito si riportano le tipologie di dati personali che sono oggetto di trattamento a seguito di una segnalazione fatta ai sensi del D.lgs. n. 24/2023

Categoria di dato personale	**Categoria di interessato**
Dati personali comuni e di contatto	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Fornitori che effettuano una segnalazione o vengono segnalati
Dati personali particolari (es. dati relativi alla salute, dati relativi all'appartenenza sindacale)	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Fornitori che effettuano una segnalazione o vengono segnalati
Dati giudiziari (es. condanne penali)	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Fornitori che effettuano una segnalazione o vengono segnalati

Ciclo di vita del trattamento dei dati (descrizione funzionale)

1) Attivazione e configurazione della piattaforma
2) Utilizzo della piattaforma – invio delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei soggetti autorizzati
3) Dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.

2.5. Risorse a supporto dei dati

Piattaforma Web Sestante.

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.
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 (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: - Processo comunicazione aziendale sull'esistenza del canale di segnalazione interno (canale informatico); - Pubblicazione sito internet – sezione dedicata al Whistleblowing
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). Nel caso invece ricorra l'ipotesi di comunicazione dei dati personali a soggetti diversi da quelli espressamente autorizzati dal Titolare, il segnalante dovrà prestare il suo consenso specifico alla segnalazione ai sensi degli, tramite piattaforma artt. 6.1. lett. a) e 7 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 l'indirizzo di posta elettronica dedicato **dpo@consorzioit.net,** 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
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 protocollo TLS 1.2 con cifrature AES128/SHA256
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.
Tracciabilità	Viene utilizzato un meccanismo di audit minimale che memorizza un identificativo dell'operatore autorizzato e la data/ora di modifica/creazione delle informazioni presenti nel database. Le operazioni effettuate dai segnalanti hanno un identificativo completamente anonimizzato (autogenerato) e legato al singolo ticket (ovvero episodio circoscritto) e non alla persona del segnalante.
Archiviazione	L'applicativo ha completo ed esclusivo controllo della base dati ed implementa al suo interno le logiche di data retention e cancellazione sicura previste dalle policy normative.
Gestione delle vulnerabilità tecniche	L'amministratore di sistema incaricato riceve bollettini di sicurezza riguardanti i moduli software in uso dall'infrastruttura ed è in grado di intervenire tempestivamente, per poter mitigare eventuali vulnerabilità critiche di recente scoperta.
Backup	Il server virtuale è ulteriormente garantito da una soluzione di Backup CDP (Continuous Data Protection) basata su R1Soft CDP. Il sistema di backup CDP effettua snapshot incrementali delle macchine virtuali con una cadenza oraria, assicurando una protezione aggiornata dei dati nel tempo senza causare interruzioni del servizio.

	Gli snapshot incrementali vengono salvati su storage server esterni Dell PowerEdge, che sono fisicamente separati dal server che ospita le macchine virtuali su networkzone distinte all'interno dello stesso datacenter. Questo approccio assicura un'adeguata sicurezza e protezione dei dati, garantendo che le copie di backup siano conservate in un ambiente separato e affidabile.
Manutenzione	L'amministratore di sistema incaricato effettua interventi almeno trimestrali (in assenza di criticità elevate) per allineare le versioni del software in uso (sia di sistema, che applicativo) con le ultime patch migliorative stabili pubblicate dai rispettivi fornitori; provvede inoltre ai passaggi di versione, laddove sopraggiungano le scadenze del supporto ufficiale dei suddetti software.
Sicurezza dei canali informatici	Tutte le connessioni sono protette tramite protocollo TLS 1.2. Le connessioni amministrative privilegiate avvengono con protocollo SSH.
Sicurezza dell'hardware	I server sono ospitati in un datacenter, situato sul territorio italiano, fisicamente isolato dove sono in essere le seguenti misure di sicurezza: - Sistema di rilevamento anti-intrusione; - Presidio con agenti di vigilanza 24 ore su 24, per sette giorni su sette; - Telecamere a circuito chiuso e archiviazione digitale delle riprese; - Sistemi di rilevamento anti-fumo, anti-incendio e anti-allagamento; - Alimentazioni multiple e indipendenti con percorsi diversificati; - Sistema di raffreddamento a doppio circuito di alimentazione; - Gruppi elettrogeni in ambienti separati; - Connettività verso internet 100Gbps multi operatore; Il provider è inoltre certificato ISO 27001:2013, ISO 14001:2015, ISO 27017:2015, ISO 27018:2019 e ha ricevuto la Certificazione dell'Agenzia per la Cybersicurezza Nazionale.
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. Gli amministratori e gli sviluppatori del prodotto operano in contesti di sicurezza conformi alle linee guida in materia, con firewall e antivirus aziendali al passo con le minacce informatiche di oggi.
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 CNIL (o altra metodologia definita dal Titolare).
Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Gli incidenti di sicurezza e le violazioni dei dati personali vengono gestiti secondo la "Procedura Data Breach" adottata dalla Società in conformità a quanto prescritto dagli artt. 33-34 del GDPR.
Vigilanza sulla protezione dei dati	Vigilanza svolta da DPO/Comitato Privacy/funzioni incaricate dal Titolare del trattamento (a secondo di quanto definito nell'organigramma privacy aziendale).

5. Rischi

5.1 Metodologia

In riferimento alla procedura "Valutazione del Rischio_Trattamenti ad Alto rischio"
Come indicato dal considerando 76, 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:

a. **Ri** è il Rischio Inerente valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione
b. **Rr** è il Rischio Residuo calcolato al netto delle misure di mitigazione del rischio (determinate in via percentuale - % abbattimento)
c. L'azienda valuta come Rischio Accettabile (**Ra**) = **3**
d. 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**

5.1 Analisi dei rischi

5.1.1. Accesso illegittimo – Perdita della riservatezza

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative, Ritorsioni.
PROBABILITÀ (P)	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

FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, 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. allagamenti, materiali pericolosi o virus informatici generici)
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

5.1.2. Modifiche indesiderate – Perdita dell'integrità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.
PROBABILITÀ (P)	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.
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, 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. allagamenti, materiali pericolosi o virus informatici generici.
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

5.1.2. Perdita del dato – Perdita della disponibilità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste

<table>
<tr><td></td><td>Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti.
Eventi simili si sono verificati molto raramente.</td></tr>
<tr><td>FONTI DI RISCHIO</td><td>Fonti umane interne (es. dipendenti, collaboratori, 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. allagamenti, materiali pericolosi o virus informatici generici.</td></tr>
<tr><td>MISURE</td><td>Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento.</td></tr>
<tr><td>CALCOLO DEL RISCHIO RESIDUO</td><td>
<table>
<tr><th>G</th><th>P</th><th>Ri</th><th>Mitigazione % abbattimento rischio</th><th>Rr</th></tr>
<tr><td>3</td><td>2</td><td>6</td><td>70%</td><td>1,8</td></tr>
</table>
</td></tr>
</table>

6. Parere delle parti interessate

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge. Ai fini dell'attivazione del canale di segnalazione interna, gli enti devono sentire le rappresentanze o le organizzazioni sindacali.

7. Parere DPO

DPO esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo.

8. 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. 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.*