Data Privacy Impact Assessment (DPIA)
Whistleblowing

MTW Holding S.p.A.
Via della Repubblica, 21
24060 Castelli Calepio (BG)
Italia

1. CONTESTO

La presente valutazione di impatto è redatta ai sensi dell'art. 13, comma 6, del D.lgs. 10 marzo 2023, n. 24, meglio noto come "Decreto Whistleblowing" (di seguito anche il "Decreto Whistleblowing").

1.1 Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi del Decreto Whistleblowing, nonché dei soggetti oggetto delle segnalazioni o, comunque, menzionati nelle segnalazioni stesse.
La gestione delle segnalazioni viene effettuata attraverso il sistema Integrity Log, adottato da MTW Holding Spa (di seguito anche la "Società"), di cui sono riportate nel presente documento le principali caratteristiche.

1.1.2. Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento: la Società
Autorizzati al trattamento: membri del Comitato Whistleblowing, incaricato della ricezione e della gestione delle segnalazioni.

1.1.3. Ci sono standard applicabili al trattamento?

Al trattamento in materia di segnalazioni ai sensi del Decreto Whistleblowing si applicano le seguenti normative e standard:
• Regolamento (UE) n. 2016/679 (il "GDPR");
• D.lgs. n. 196/2003 (il "Codice Privacy"), così come modificato dal D.lgs. n. 101/2018;
• Direttiva UE 2019/1937 (la "Direttiva Whistleblowing");
• Decreto Whistleblowing.
Sono state inoltre tenuti in considerazione i principi di cui alle "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." approvate dall'Autorità Nazionale Anticorruzione (ANAC) con Delibera n°311 del 12 luglio 2023 e ss.

1.2. Dati, processi e risorse di supporto

1.2.1. Dati trattati

I dati personali raccolti e oggetto di trattamento in caso di segnalazioni effettuate ai sensi del Decreto Whistleblowing:
• dati personali comuni e di contatto (in particolare, informazioni sulla propria identità, nome e cognome, paese di residenza, numero di telefono o indirizzo e-mail);
• dati personali particolari: in linea di principio, non sono richiesti né trattati dati personali appartenenti ad alcuna categoria particolare (ad esempio, informazioni sull'origine razziale e/o etnica, convinzioni religiose e/o ideologiche, appartenenza sindacale o orientamento sessuale);
• dati giudiziari (es. condanne penali): in linea di principio, non sono richiesti né trattati dati appartenenti a questa categoria, i quali, tuttavia, potrebbero essere volontariamente comunicati dagli interessati, a causa di campi di testo libero nel modulo di registrazione.
I dati sopra indicati si riferiscono alle seguenti categorie di interessati:
• soggetti segnalanti, così come individuati dal Decreto Whistleblowing;
• soggetti che siano oggetto della segnalazione o comunque menzionati nella segnalazione stessa.

1.2.2. Qual è il 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;
• ricezione e gestione delle segnalazioni da parte dei soggetti autorizzati;
3) dismissione della piattaforma (nei termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.

1.2.3. Quali sono le risorse di supporto ai dati?

Piattaforma Integrity Log, ospitata sul sito internet aziendale.

2. PRINCIPI FONDAMENTALI

2.1. Proporzionalità e necessità

2.1.1. Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento è finalizzato esclusivamente alla ricezione e alla gestione delle segnalazioni effettuate ai sensi del Decreto Whistleblowing.

2.1.2. Quali sono le basi giuridiche che rendono lecito il trattamento?

Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge derivante dalle previsioni di cui al Decreto Whistleblowing e alla Direttiva Whistleblowing, la cui osservanza è condizione di liceità del trattamento ai sensi dell'art. 6, par. 1, lett. c) del GDPR.
I dati potranno inoltre essere trattati sulla base del consenso dell'interessato nelle ipotesi previste dal Decreto Whistleblowing.
Nel caso in cui, in sede di compilazione della segnalazione o nella successiva procedura di indagine, venissero forniti dati personali appartenenti a categorie particolari, tali dati saranno trattati sulla base di quanto previsto dall'art. 9, comma 2, lettere b) e f) del GDPR.

2.1.3. I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

In conformità al principio di minimizzazione previsto dal GDPR, i dati personali raccolti sono solo quelli espressamente necessari alla ricezione e alla gestione della segnalazione.

2.1.4. I dati sono esatti e aggiornati?

I dati personali relativi alle segnalazioni sono esatti e aggiornati, in quanto forniti direttamente dai soggetti interessati in occasione dell'invio della segnalazione. Inoltre, i soggetti autorizzati a ricevere e gestire le segnalazioni ne verificano, per quanto possibile, preliminarmente la corrispondenza a verità.
In ipotesi di decorrenza di un lungo periodo tra la segnalazione e il processo di gestione sella stessa, i gestori provvederanno a verificare l'aggiornamento dei dati.

2.1.5. Qual è il periodo di conservazione dei dati?

Conformemente a quanto previsto dall'art. 14 del Decreto Whistleblowing, le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e, comunque, non oltre cinque anni, decorrenti dalla data di comunicazione dell'esito finale della procedura di segnalazione, decorsi i quali i dati saranno cancellati, fatta salva l'eventuale necessità di conservazione per un periodo ulteriore al fine di adempiere ad obblighi di legge o ordini dell'Autorità.

2.2. Misure a tutela dei diritti degli interessati

2.2.1. Come sono informati del trattamento gli interessati?

Gli interessati sono informati attraverso una specifica informativa ai sensi degli artt. 13 del GDPR, resa disponibile secondo le seguenti modalità:
- video distribuito a tutti i dipendenti aziendali
- affissione sulla bacheca aziendale

2.2.2. Come si ottiene il consenso degli interessati, ove applicabile?

Il trattamento dei dati personali relativi alle segnalazioni di regola non necessita di consenso da parte dell'interessato posto che la sua base giuridica è rinvenibile nell'adempimento di un obbligo di legge, ai sensi dell'art. 6, par .1, lett. c) del GDPR.
Nei casi, invece, in cui, ai sensi del Decreto Whistleblowing sia richiesto il consenso dei soggetti interessati (ad esempio, nell'ipotesi di comunicazione dei dati personali a soggetti diversi da quelli espressamente autorizzati dal Titolare), tale consenso dovrà essere prestato, in modo specifico, tramite la piattaforma, conformemente a quanto previsto dal GDPR.

2.2.3. Come fanno gli interessati a esercitare i loro diritti previsti dagli artt. 15 ss. del GDPR?

Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR a mezzo lettera raccomandata indirizzata alla Società o via e-mail, all'indirizzo di posta elettronica mtwholding@legalmail.it.

2.2.4. 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 un contratto in cui sono definiti con chiarezza gli obblighi reciproci gravanti sulle parti.

2.2.5. 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 al di fuori dell'Unione Europea.

3. MISURE ESISTENTI

3.1. Panoramica

Il sistema adottato dalla Società e oggetto di disamina consiste in un canale di segnalazione che consente ai segnalanti di inviare le proprie segnalazioni in merito a eventuali presunti illeciti e violazioni della legge e che possono concretizzarsi nel compimento di un reato.
Le segnalazioni vengono ricevute attraverso un sistema integrato di gestione dei casi che consente ai membri del Comitato Whistleblowing di esaminare e indagare sulle segnalazioni in modo strutturato, fornendo strumenti per l'indagine.
Il sistema viene fornito come Software as a Service (SaaS), il che significa che per utilizzarlo sono necessari solo un browser web e una connessione a Internet.
Il canale di segnalazione (Web Intake) per l'invio delle segnalazioni è ottimizzato per i dispositivi mobili (progressive web app / PWA).

Tutti i canali di segnalazione supportano una comunicazione sicura e bidirezionale tra il Comitato Whistleblowing e il segnalante.
Per poter salvaguardare i dati sensibili, sono state implementate le relative tecnologie di miglioramento della privacy (PET) (privacy by design). Nel presente paragrafo 3 sono riassunte le varie tecnologie impiegate dall'applicazione, al fine di conformare il trattamento dei dati alle disposizioni di cui al GDPR (minimizzazione dei dati, anonimizzazione, impostazioni predefinite, trasparenza, algoritmi crittografici, ecc.).
L'analisi dettagliata di tali tecnologie, del Sistema di gestione della sicurezza delle informazioni (ISMS), della Sicurezza delle reti e delle applicazioni e della sicurezza dei dati (crittografia, dati memorizzati, trasmissione dei dati, gestione delle chiavi di crittografia) sono contenuti nella descrizione tecnica della piattaforma, che è allegata al presente documento (all. 1) e forma parte integrante dello stesso.

4. ANALISI DEI RISCHI

4.1. Possibili rischi

Sono configurabili i seguenti rischi:
• accesso illegittimo ai dati (perdita della riservatezza);
• modifiche indesiderate dei dati (perdita dell'integrità);
• perdita di dati (perdita della disponibilità).

4.2. Quali potrebbero essere i principali impatti sugli interessati se i rischi si dovessero concretizzare? Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Se i rischi suddetti dovessero concretizzarsi, in capo ai soggetti interessati potrebbero verificarsi conseguenze significative, ma comunque superabili, quali, ad esempio: disagio, diffusione indesiderata dei propri dati, consultazione dei propri da parte di personale non autorizzato, problematiche di natura giuslavoristica e contrattuale, mobbing, discriminazioni lavorative, ritorsioni.

4.3. Quali sono le fonti di rischio?

• Fonti umane interne (es. dipendenti o collaboratori, la cui condotta può essere accidentale o intenzionale);
• Fonti umane esterne (es. fornitori, la cui condotta può essere accidentale o intenzionale; hacker);
• Fonti non umane (es. virus informatici).

4.4. Quali misure, tra quelle individuate, contribuiscono a mitigare il rischio?

Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 3 del presente documento e all'allegato 1 e afferiscono sia a misure di natura organizzativa (inclusa l'attività informativa e formativa) che di natura informatica. Inoltre, la Società procederà a tenere sotto costante monitoraggio l'efficacia di tali misure anche a mezzo di possibili audit sia esterni (es. il Responsabile del trattamento) o interni.

4.5. Come stimereste la probabilità e l'impatto del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Il verificarsi del danno dipende da condizioni impreviste e si può ipotizzare che risulti poco probabile. In ogni caso, anche in relazione alle misure di sicurezza adottate e alle procedure in essere nonché alla formazione che verrà effettuata di ritiene che l'impatto di un improbabile rischio risulti tendenzialmente limitato.

Allegati:

1. Descrizione tecnica della piattaforma_____

MTW Holding S.p.A.
MTW HOLDING S.P.A.
Via Della Repubblica n.21/A
24060 Castelli Calepio (BG)
P.IVA e C.F. 04325720169