DATA PRIVACY IMPACT ASSESSMENT (DPIA)

Ai sensi dell'art. 35 del Regolamento UE n. 679/2016 (GDPR) e dell'art. 13, c. 6, del D. Lgs. n. 24/2023 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali (Decreto Whistleblowing)

Versione del 22/01/2025

1. Premessa

La Valutazione di Impatto sulla Protezione dei Dati (*Data Protection Impact Assessment* – "**DPIA**") è una procedura finalizzata a descrivere un trattamento di dati personali allo scopo di valutarne la necessità e la proporzionalità, nonché gestirne eventuali rischi associati ai diritti e alle libertà delle persone fisiche coinvolte. Tale valutazione prevede una stima del livello di rischio e la determinazione di misure atte a mitigarlo. La DPIA rappresenta uno strumento essenziale e fondamentale nell'ambito dell'attuazione dell'approccio alla protezione dei dati personali previsto dal Regolamento UE n. 679/2016 (GDPR), basato ampiamente sul principio della responsabilizzazione (*accountability*).

Conformemente all'articolo 35 del GDPR, la DPIA è obbligatoria quando il trattamento dei dati personali "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" e, in particolare, quando il trattamento implichi:

(a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
(b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del GDPR o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR;
(c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Per i trattamenti oggetto della presente DPIA, l'obbligo di svolgere la valutazione è stato esplicitamente stabilito dal legislatore nel D. Lgs. n. 24/2023 (Decreto Whistleblowing), all'art. 13, comma 6: "*I soggetti* [obbligati] *definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati,* ***sulla base di una valutazione d'impatto sulla protezione dei dati*** (…)".

Ai sensi dell'art. 35 del GDPR, poi, la DPIA deve contenere almeno:

(a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
(b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
(c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
(d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Si precisa, infine, che la presente DPIA è stata integrata con la metodologia di analisi dei rischi adottata dal CNIL (*Autorità Garante Francese per la protezione dei dati personali*).

2. Contesto

In questa fase della DPIA viene elaborata una descrizione sistematica del trattamento, dei soggetti coinvolti e degli elementi di caratterizzazione del trattamento, con lo scopo di individuare le tipologie di dati, il loro ciclo di vita, le modalità e gli strumenti del trattamento, nonché i sistemi impiegati e le risorse di supporto.

2.1. Panoramica del trattamento

Qual è il trattamento in considerazione?

Trattamento dei dati personali, potenzialmente anche appartenenti a categorie particolari, degli interessati che utilizzano i canali di segnalazione interna (whistleblowing) messi a disposizione dalla Società.

Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento è **NOVIT INNOVAZIONE E TECNOLOGIE S.P.A.** con sede in Milano, Via Gaetano Giardino 1, codice fiscale, Partita IVA e numero di iscrizione al Registro delle Imprese di Milano nr. 05396760968.

NOVIT ha conferito l'incarico di *DPO* a **BRIOLA&PARTNERS S.R.L.**, con sede in Via Podgora n. 11, 20122 Milano (MI), P.IVA 10579350967, con referente individuato nell'AVV. MARIKA FARDO. Il *DPO* è raggiungibile ai seguenti contatti: e-mail dpo@l22.it, T. +39 0255180585, F. + 39 0255182047.

ZUCCHETTI S.P.A., P.IVA 05006900962, quale fornitore della piattaforma è responsabile del trattamento ex art. 28 GDPR.

Al fine di garantire l'autonomia e l'imparzialità nella gestione dei canali di segnalazione interni, la stessa è stata affidata ad un Soggetto esterno, AVV. MONICA DEL GROSSO formalmente nominata, ex art. 28 del GDPR, responsabile del trattamento.

Il Gestore, quale membro di un organismo della Società dotato di autonomia garantisce (i) l'assenza di interferenze nella gestione delle segnalazioni e (ii) il rispetto della riservatezza dell'identità del segnalante, delle persone coinvolte o comunque menzionate e dell'eventuale documentazione allegata alla segnalazione.

Il Gestore, nella sua qualità di responsabile del trattamento elabora i dati personali di cui alle segnalazioni per conto del titolare del trattamento e in base alle sue istruzioni documentate.

Ci sono standard applicabili al trattamento?

- **Principi fondamentali del GDPR**: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza dei dati.
- **Requisiti specifici richiesti dal D. Lgs. 24/2023**: rispetto dei principi di cui agli artt. 5 e 25 del GDPR, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento, nonché adozione di misure appropriate a tutela dei diritti e delle libertà degli interessati.
- **ENISA Whistleblowing – *An inventory of risk management and good practice***: linee guida fornite dall'Agenzia Europea per la Sicurezza delle Reti e delle Informazioni (ENISA) per la gestione dei rischi e della sicurezza dei dati nel contesto del whistleblowing;
- **Linee Guida del Garante Europeo e del Garante Nazionale;**
- **Linee Guida dell'Autorità Nazionale Anti-Corruzione (ANAC)**.

2.2. Dati, processo e risorse di supporto

Quali sono i dati trattati?

L'invio, la ricezione e la gestione delle segnalazioni possono dar luogo a trattamenti di dati personali c.d. comuni (nome, cognome, ruolo lavorativo, numero di telefono, indirizzo e-mail, ecc.) nonché, a seconda del contenuto delle segnalazioni e dei documenti a queste eventualmente allegati, a trattamenti di dati personali c.d. "*particolari*" (ad es., dati relativi a condizioni di salute, orientamento sessuale o appartenenza sindacale, di cui all'art. 9 GDPR) e di dati personali *relativi a condanne penali e reati* (di cui all'art. 10 GDPR).

I dati personali sono acquisiti in quanto contenuti nella segnalazione e/o in documenti a questa eventualmente allegati e possono riferirsi sia al soggetto segnalante che ad altre persone, indicate come possibili responsabili delle violazioni o, comunque, a vario titolo coinvolte nelle vicende segnalate.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

I dati vengono raccolti nelle seguenti circostanze:

(i) Invio della segnalazione mediante Piattaforma My Whistleblowing;

(ii) Analisi delle segnalazioni;

(iii) Investigazione delle segnalazioni, se fondate e pertinenti;

(iv) Azioni in conseguenza delle segnalazioni.

La raccolta dei dati personali può avvenire direttamente presso l'interessato segnalante ovvero tramite altri soggetti che potrebbero essere coinvolti dal Gestore per dare corretto seguito alla segnalazione.

Quali sono le risorse di supporto ai dati?

Il sistema è gestito mediante piattaforma MY WHISTLEBLOWING di Zucchetti S.p.A.

3. Principi fondamentali

In questa fase della DPIA è svolta l'analisi della necessità e della proporzionalità del trattamento dei dati personali e la verifica della conformità del trattamento ai principi fondamentali del GDPR, con particolare riferimento a: basi giuridiche del trattamento, applicazione del principio di minimizzazione dei dati personali trattati, periodo di conservazione dei dati e compatibilità con il principio di limitazione della conservazione, completezza e chiarezza delle informazioni rese agli interessati, procedure per l'esercizio dei diritti, misure di sicurezza da implementare, specifici obblighi imposti ai responsabili del trattamento e alle altre parti coinvolte nel trattamento dei dati.

3.1. Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento dei dati sono specifiche, esplicite e legittime. Le finalità sono precisate al momento della raccolta dei dati personali e sono conformi agli obblighi legislativi citati nelle Premesse.

In particolare, il Gestore e il Titolare provvedono al trattamento dei dati personali forniti al momento della presentazione di una segnalazione di violazione per le seguenti finalità:

a) Ricezione, istruttoria e gestione della segnalazione;
b) Istruttoria per eventuali provvedimenti successivi (azione disciplinare o giudiziaria).

Quali sono le basi giuridiche che rendono lecito il trattamento?

Per le sopra esposte finalità:

(a) il trattamenti dei dati "comuni" si fonda sull'*adempimento di un obbligo legale al quale è soggetto il titolare del trattamento*, ai sensi dell'art. 6, par. 1, lett. c) del GDPR;
(b) il trattamento dei dati "particolari" si fonda sull'*assolvimento degli obblighi e sull'esercizio di diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro*, ai sensi dell'art. 9, par. 2, lett. b), del GDPR;
(c) il trattamento dei dati relativi a condanne penali o reati si fonda sull'*adempimento di un obbligo legale al quale è soggetto il titolare del trattamento*, ai sensi dell'art. 6, par. 1, lett. c) del GDPR.

Costituisce, infatti, obbligo del Titolare ai sensi del D. Lgs. 24/2023 (i) permettere ai soggetti legittimati di segnalare eventuali violazioni di cui siano venuti a conoscenza nell'ambito del proprio rapporto di lavoro; (ii) mantenere le interlocuzioni con i segnalanti; (iii) dare un corretto seguito alle segnalazioni; e (iv) fornire riscontro alle segnalazioni.
L'eventuale rivelazione dell'identità del segnalante al segnalato ovvero la comunicazione dei relativi dati personali a soggetti terzi eventualmente coinvolti nella gestione della segnalazione è fondata sul consenso del segnalante.

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 e trattati sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dal D.lgs. n. 24/2023.
Il perseguimento delle finalità avviene, pertanto, nel rispetto del principio di minimizzazione (art. 5.1. lett. c) GDPR).

I dati sono esatti e aggiornati?

I dati sono esatti e mantenuti costantemente aggiornati dai soggetti autorizzati al trattamento (Gestore e altri soggetti potenzialmente coinvolti).

Qual è il periodo di conservazione dei dati?

Ai sensi dell'art. 14 del D. Lgs. 24/2023, le segnalazioni interne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 (cinque) anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza e dei principi di cui all'art. 5, par. 1, lett. e) del GDPR.

3.2. Misure a tutela dei diritti degli interessati

Come sono informati gli interessati al trattamento?

I soggetti interessati sono informati del trattamento mediante a specifica informativa redatta ai sensi degli artt. 13 e 14 del GDPR (i) esposta e resa facilmente visibile nei luoghi di lavoro; (ii) pubblicata sul sito aziendale.

Ove applicabile: come si ottiene il consenso degli interessati?

Il trattamento dei dati personali relativo alla procedura di segnalazione **non necessita di consenso** da parte degli interessati, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (art. 6, par. 1, lett. c) o art. 9, par. 2, lett. b) del GDPR), fatto salvo il caso di rivelazione dell'identità del segnalante al segnalato ovvero la comunicazione dei relativi dati personali a

soggetti terzi eventualmente coinvolti nella gestione della segnalazione è fondata sul consenso del segnalante. In queste ipotesi, è cura del Gestore raccogliere il consenso dell'interessato.

Come fanno gli interessati ad esercitare i diritti loro garantiti dagli artt. 15 e seguenti del GDPR?

Gli interessati possono esercitare i diritti previsti dagli artt. 15 e ss. del GDPR utilizzando i seguenti recapiti: amministrazione@novit.it

In deroga a quanto sopra, ai sensi dell'art. 2-*undecies* del D. Lgs. 196/2003, si precisa che la persona coinvolta e la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione (così come di una divulgazione pubblica o di una denuncia), non possono esercitare i diritti che normalmente il GDPR riconosce agli interessati, in quanto dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante. In tali casi, dunque, al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al Titolare e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante per la protezione dei dati personali.

Gli obblighi degli incaricati al trattamento e dei responsabili del trattamento sono definiti con chiarezza e disciplinati in un contratto?

In conformità con le tutele previste dal D. Lgs. 24/2023 e con particolare riguardo alla tutela della riservatezza del segnalante, i dati personali degli interessati sono trattati esclusivamente dal soggetto esterno (quale Gestore) nominato Responsabile esterno del trattamento ex art. 28 GDPR**.**

Il fornitore della piattaforma online (My Whistleblowing) è stato nominato Responsabile esterno del trattamento ex art. 28 GDPR.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Con riferimento ai canali (scritto e orale) interni alla Società, i dati personali raccolti non sono oggetto di trasferimento verso Paesi non appartenenti all'Unione Europea (c.d. Paesi terzi). Con riferimento alla piattaforma My Whistleblowing, il fornitore garantisce che tutti i dati e documenti sono conservati e gestiti su server certificati Microsoft Azure in UE.

4. Rischi

In questa fase vengono stimati i rischi per gli interessati derivanti dal trattamento dei dati personali oggetto della DPIA, in termini di probabilità di accadimento della violazione dei dati personali e di gravità/impatto degli effetti della violazione.
In particolare, l'attività di individuazione e verifica del rischio intrinseco al trattamento dei dati personali oggetto della presente DPIA consiste nella valutazione oggettiva, qualitativa e preliminare degli effetti complessivi del trattamento, seguendo i seguenti principali passaggi:

A. **ANALISI DEI TRATTAMENTI DATI PERSONALI DELLA SOCIETÀ**: identificazione dei trattamenti dei dati personali operati dalla Società e delle relative principali caratteristiche (e.g. finalità, tipologia e categoria di dati personali, categorie di interessati, durata del trattamento, trasferimenti dei dati personali all'estero ecc.).

B. **ANALISI DEI DIRITTI E DELLE LIBERTÀ DEGLI INTERESSATI E DEL RELATIVO IMPATTO**: individuazione dei diritti e libertà degli interessati che possono essere limitati o pregiudicati dal trattamento dei dati personali operato dalla Società e successiva verifica dell'impatto negativo causato dalla possibile limitazione e/o dal pregiudizio ai diritti e libertà degli interessati. Tale impatto negativo è in grado di cagionare "*un danno fisico, materiale o immateriale […] o qualsiasi altro danno economico o sociale significativo*", agli interessati (cfr. Considerando 75 del Regolamento). A titolo esemplificativo, i danni possono essere rappresentati da: impossibilità di utilizzare servizi o prodotti, lesioni alla reputazione, discriminazione, furto di identità, perdite finanziarie, danni fisici o psicologici, perdita di controllo dei dati e altri svantaggi economici o sociali.

C. **ANALISI DELLA GRAVITÀ DELL'IMPATTO:** la valutazione della gravità dell'impatto è svolta sulla base di una serie di parametri, quali la tipologia e la quantità di dati personali (e.g. eventuali categorie particolari di dati personali e/o dati giudiziari, tipologia di profili degli interessati, mole di dati nei sistemi della società), le eventuali criticità delle operazioni che costituiscono il trattamento, specifiche caratteristiche del titolare o del responsabile (e.g. sede legale o operativa extra SEE), specifiche caratteristiche degli interessati (e.g. minori, pazienti, richiedenti asilo) e il livello di identificabilità degli interessati (e.g. eventuali pseudonimizzazione). In via preliminare, l'impatto viene verificato complessivamente per ogni trattamento e viene classificato secondo i livelli di cui alla seguente tabella.

Livello di impatto	Descrizione
Basso	Gli interessati possono incontrare pochi e minimi inconvenienti, che possono superare senza problemi (e.g. perdita di tempo nel reinserimento di informazioni, seccature, fastidi, ecc.)
Medio	Gli interessati possono incontrare significativi inconvenienti, che possono essere in grado di superare nonostante alcune difficoltà (e.g. costi extra, impedimento ad accedere ad alcuni servizi, mancanza di comprensione, stress, ecc.)
Elevato	Gli interessati possono incontrare significativi pregiudizi, che possono essere in grado di superare nonostante serie difficoltà (e.g. furto di identità, perdita di fondi, perdita del lavoro, danni a beni posseduti, aggravamenti dello stato di salute ecc.)

D. **IDENTIFICAZIONE DELLE POSSIBILI MINACCE E DELLA RELATIVA PROBABILITÀ DI ACCADIMENTO**: identificazione delle fonti delle minacce, tenendo conto delle fonti umane interne alla Società (e.g. dipendenti o interessati), delle fonti umane esterne alla Società (e.g. soggetti terzi) e delle fonti non umane (e.g. virus informatici o incendi) e conseguente classificazione delle minacce in eventi colposi o dolosi o eventi accidentali. La probabilità si definisce per ciascun trattamento, nel suo complesso, secondo i livelli di cui alla seguente tabella.

Livello di probabilità	Descrizione
Bassa	È improbabile che la minaccia si materializzi
Medio	È possibile che la minaccia si materializzi
Elevato	È probabile che la minaccia si materializzi

E. **VALUTAZIONE DEL LIVELLO DEL RISCHIO DI OGNI TRATTAMENTO:** dopo aver valutato la gravità dell'impatto e la probabilità di accadimento delle minacce, per ogni singolo trattamento dei dati personali, il livello di rischio viene determinato in base al rapporto tra i livelli di cui alle precedenti tabelle di cui alle lettere C e D, come di seguito descritto.

		Livello di gravità dell'impatto		
		Basso	Medio	Elevato
	Bassa			

Livello di probabilità delle minacce	**Medio**			
	Elevato			

In particolare, per il trattamento di dati personali di cui alla presente DPIA, è possibile distinguere tre scenari di rischio:

(i) **Accesso non autorizzato ai dati**, derivante da una potenziale violazione della riservatezza, ovvero dalla divulgazione o dall'accesso non autorizzato o accidentale ai dati personali;

(ii) **Modifiche indesiderate dei dati**, dovute a possibili violazioni dell'integrità, ovvero alla modifica non autorizzata o accidentale dei dati personali;

(iii) **Perdita di dati**, risultante da una possibile violazione della disponibilità, ovvero dalla perdita o dalla distruzione accidentale o non autorizzata dei dati personali.

4.1. Misure esistenti o pianificate

Controllo degli accessi logici
- Identificazione degli incaricati al trattamento;
- Assegnazione di credenziali di accesso alla rete differenziate per servizio/server/gestionali/posta elettronica;
- Credenziali di accesso costituite da un codice per l'identificazione dell'utente (username) ed una password;
- Modifica password a cura dell'utente al primo accesso ed aggiornamento periodico;
- Definizione di regole per la scelta delle password;
- Limitazione degli accessi ai dati (minimizzazione);
- Controllo degli accessi a hardware, software ed archivi elettronici (*log*);
- Utilizzo di salvaschermo protetti da password in caso di inattività.

Backup
- Effettuazione di copie di sicurezza;
- Backup centralizzato periodico;
- Istruzioni su backup proceduralizzate internamente.

Controllo degli accessi fisici
- Conservazione dei documenti cartacei in archivi (armadi) ad accesso controllato;
- I locali contenenti gli archivi sono chiusi a chiave;
- Le chiavi degli archivi e dei locali sono consegnate solo al personale autorizzato;
- I dati particolari in formato cartaceo sono conservati separatamente dagli altri dati personali;
- Monitoraggio degli accessi alle strutture (presenza di sistemi di videosorveglianza esterni e/o interni);
- I server sono localizzati in strutture dedicate e con elevati livelli di sicurezza.

Protezione contro fonti di rischio non umane
- Dotazione di dispositivi antincendio;
- Continuità dell'alimentazione elettrica.

Politica di tutela della privacy

- Nomina di incaricati al trattamento e responsabili del trattamento;
- Redazione di procedure a tutela della riservatezza dei segnalanti, delle persone coinvolte e delle persone comunque menzionate, nonché della documentazione eventualmente allegata;
- Redazione di specifiche informative ai sensi degli artt. 13 e 14 del GDPR;
- Interventi e corsi per i dipendenti dedicati alla formazione in tema di privacy e protezione dei dati personali.

Garanzie fornite dal fornitore della piattaforma My Whistleblowing

- My Whistleblowing assicura la riservatezza del segnalante e del contenuto della segnalazione utilizzando la crittografia AES 256.
- La piattaforma permette di gestire automaticamente la retention delle segnalazioni rispettando i criteri stabiliti dal Decreto.
- I gestori delle segnalazioni possono scambiarsi informazioni riservatamente su ogni singola segnalazione tutelando sempre i dati del segnalante.
- Il software è completamente autonomo per assicurare che il dipartimento IT dell'azienda non possa accedere in alcun modo alle segnalazioni.
- La piattaforma non traccia l'accesso all'applicativo e separa il contenuto della segnalazione dall'identità del segnalante.
- Soddisfa gli standard nazionali e internazionali sulla protezione dei dati come il GDPR.

4.1. Accesso illegittimo ai dati – Perdita della riservatezza

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

In considerazione delle misure di sicurezza implementata dalla Società, la valutazione del rischio può essere così schematizzata:

Livello gravità impatto	Livello probabilità minacce	Rischio
Medio	**Basso**	**Medio**

Rischio medio – gli interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: disagio, diffusione indesiderata dei propri dati, consultazione dei propri dati da parte di personale non autorizzato, problematiche di natura giuslavoristica e contrattuale, mobbing, discriminazioni lavorative, ritorsioni.

Inoltre, lo specifico rischio è mitigato dalle tutele previste dal Decreto Whistleblowing e, in particolare, dal generale divieto di ritorsione di cui all'art. 17 e dalle misure a protezione dalle ritorsioni di cui all'art. 19.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Problemi tecnici: anomalie e malfunzionamenti dei software, hardware o di altre componenti della rete informatica;

- Compromissione delle informazioni: intercettazioni, rivelazioni, infiltrazioni nella posta elettronica, ecc.;
- Azioni non autorizzate: errori volontari o involontari, virus, accesso non autorizzato alle informazioni.

Quali sono le fonti di rischio?

- Fonti umane interne;
- Fonti umane esterne.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Backup, Controllo degli accessi fisici, Politica di tutela della privacy, Gestione del personale, Sicurezza dei canali informatici, accordi di nomina a responsabile esterno, Garanzie fornite dal fornitore della piattaforma My Whistleblowing.

4.2. Modifiche indesiderate ai dati – Perdita dell'integrità

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

In considerazione delle misure di sicurezza implementata dalla Società, la valutazione del rischio può essere così schematizzata:

Livello gravità impatto	Livello probabilità minacce	Rischio
Medio	**Basso**	**Medio**

Rischio medio – gli interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: disagio, diffusione indesiderata dei propri dati, consultazione dei propri dati da parte di personale non autorizzato, problematiche di natura giuslavoristica e contrattuale, mobbing, discriminazioni lavorative, ritorsioni.

Inoltre, lo specifico rischio è mitigato dalle tutele previste dal Decreto Whistleblowing e, in particolare, dal generale divieto di ritorsione di cui all'art. 17 e dalle misure a protezione dalle ritorsioni di cui all'art. 19.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Problemi tecnici: anomalie e malfunzionamenti dei software, hardware o di altre componenti della rete informatica;
- Compromissione delle informazioni: intercettazioni, rivelazioni, infiltrazioni nella posta elettronica, ecc.;

- Azioni non autorizzate: errori volontari o involontari, virus, accesso non autorizzato alle informazioni.

Quali sono le fonti di rischio?

- Fonti umane interne;
- Fonti umane esterne;
- Fonti non umane (allagamenti, virus informatici generici, ecc.).

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Backup, Controllo degli accessi fisici, Politica di tutela della privacy, Gestione del personale, Sicurezza dei canali informatici, accordi di nomina a responsabile esterno, Garanzie fornite dal fornitore della piattaforma My Whistleblowing.

4.3. Perdita del dato

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

In considerazione delle misure di sicurezza implementata dalla Società, la valutazione del rischio può essere così schematizzata:

Livello gravità impatto	Livello probabilità minacce	Rischio
Medio	**Basso**	**Medio**

Rischio medio – gli interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: disagio, diffusione indesiderata dei propri dati, consultazione dei propri dati da parte di personale non autorizzato, problematiche di natura giuslavoristica e contrattuale, mobbing, discriminazioni lavorative, ritorsioni.

Inoltre, lo specifico rischio è mitigato dalle tutele previste dal Decreto Whistleblowing e, in particolare, dal generale divieto di ritorsione di cui all'art. 17 e dalle misure a protezione dalle ritorsioni di cui all'art. 19.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Problemi tecnici: anomalie e malfunzionamenti dei software, hardware o di altre componenti della rete informatica;
- Compromissione delle informazioni: intercettazioni, rivelazioni, infiltrazioni nella posta elettronica, ecc.;

- Azioni non autorizzate: errori volontari o involontari, virus, accesso non autorizzato alle informazioni.

Quali sono le fonti di rischio?

- Fonti umane interne;
- Fonti umane esterne;
- Fonti non umane (allagamenti, virus informatici generici, ecc.).

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Backup, Controllo degli accessi fisici, Politica di tutela della privacy, Gestione del personale, Sicurezza dei canali informatici, accordi di nomina a responsabile esterno, Garanzie fornite dal fornitore della piattaforma My Whistleblowing.

5. Parere delle parti interessate

Non è stato richiesto un parere alle parti interessate in quanto il trattamento dei dati personali è effettuato in adempimento di un obbligo di legge.

6. Conclusioni

La DPIA relativa ai trattamenti di dati personali degli interessati che utilizzano i canali di segnalazione interna della Società conferma che, nonostante il trattamento di dati personali potenzialmente anche appartenenti a categorie particolari, il rischio associato a tale trattamento non è elevato.

Difatti, la Società ha:

(i) implementato misure di sicurezza adeguate a ridurre al minimo i rischi per i diritti e le libertà degli interessati;

(ii) affidato la gestione del canale di segnalazione interna ad un soggetto dotato dei caratteri di autonomia e competenza previsti dal D. Lgs. 24/2023.

Pertanto, si ritiene che il trattamento in oggetto presenti un grado di rischio sui diritti e libertà degli interessati rientrante in parametri accettabili e, di conseguenza, non è richiesta una consultazione preventiva dell'Autorità Garante.

NOVIT INNOVAZIONE E TECNOLOGIE S.P.A.

Il legale rappresentante _____

Parere del D.P.O.:

Considerato che il trattamento di dati personali in oggetto costituisce adempimento di un obbligo legale ai sensi del D.lgs. n. 24/2023 e che la Società ha adottato una piattaforma digitale che presenta sufficienti garanzie di adeguatezza, si ritiene che il trattamento in oggetto presenti un grado di rischio sui diritti e libertà degli interessati rientrante in parametri accettabili e, di conseguenza, non è richiesta una consultazione preventiva dell'Autorità Garante.

BRIOLA&PARTNERS S.R.L. – S.T.A.

Il referente interno – Avv, Marika Fardo

_____