ENTSORGA ITALIA SPA

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI AI SENSI DELL'ART. 35 GDPR

Rev.	Data	Descrizione	Scritto	Controllato	Approvato
0	20/12/23	Prima emissione	Zani	SM/Zani	DIR

Sommario

1 SEZIONE 1: CONTESTO

Questa sezione permette una visione complessiva del trattamento o dei trattamenti di dati personali in questione.

Sottosezione 1.1: Panoramica del trattamento

Questa sezione permette di individuare e presentare l'oggetto dell'analisi.

1.1.1. Quale è il trattamento in considerazione?

Il trattamento "Whistleblowing" consiste nella trattazione dei dati personali di cui alle segnalazioni che pervengono alla società nel contesto dell'apposito canale di whistleblowing adottato a norma del D.L.vo n°24 del 2024.

Lo scopo del trattamento risiede nella corretta gestione delle segnalazioni, che comprende le seguenti fasi: valutazione della fondatezza della segnalazione; approfondimento sui comportamenti segnalati; reporting agli organi sociali e/o alle pubbliche Autorità; riscontro al segnalante.

1.1.2. Quali sono le responsabilità connesse al trattamento?

Il Titolare del trattamento è Entsorga Italia S.p.A.

Gli Incaricati del trattamento sono: i dipendenti della società a cui l'Organismo di Vigilanza (v. successivo capoverso) può rivolgersi nel corso della gestione della segnalazione per acquisire informazioni.

I Responsabili del trattamento sono: l'Organismo di Vigilanza adottato dalla società a norma del D.L.vo n°231 del 2001, che funge da gestore delle segnalazioni; eventuali professionisti esterni alla società a cui l'OdV può rivolgersi nel corso della gestione della segnalazione per acquisire informazioni o consulenze.

1.1.3. Ci sono standard applicabili al trattamento?

Si applicano i principi di cui al capo II del Reg. UE 2016/679 (GDPR).
I diritti degli Interessati possono essere limitati ai sensi dell'art. 2 undecies, comma 1, lett. 'f', del D.L.vo n°196 del 2003.

Sottosezione 1.2: Dati, processi e risorse di supporto

Questa sezione permette di definire e descrivere nei dettagli il trattamento in oggetto.

1.2.1. Quali sono i dati trattati?

I dati raccolti sono:

a) dati personali comuni ai sensi dell'art. 4 GDPR del segnalante, delle persone coinvolte o comunque menzionate nella segnalazione, del facilitatore. Tali dati possono consistere in: dati anagrafici, dati di contatto, dati relativi all'occupazione, dati finanziari ed economici, fatti, atti ed altri contenuti della segnalazione.
b) dati appartenenti alle categorie particolari di cui all'art. 9 GDPR se inevitabile e necessario per la corretta gestione della segnalazione.

Gli Interessati sono quindi: i segnalanti, le persone coinvolte o menzionate nella segnalazione, i facilitatori ai sensi del D.L.vo n°24 del 2023. I segnalanti, a norma del D.L.vo n°24 del 2023, possono essere i dipendenti della società, i collaboratori ed i professionisti esterni alla società che intrattengono con essa rapporti di affari

(contratti di collaborazione, d'opera professionale e simili), i volontari e tirocinanti della società, gli amministratori della società. I facilitatori sono persone che aiutano il segnalante ad eseguire la segnalazione e che opera nel medesimo contesto lavorativo.
Non è previsto il trattamento di dati relativi a interessati potenzialmente vulnerabili o che difficilmente siano in grado di far valere i propri diritti (ad esempio minori, anziani, pazienti, ecc.).

Il periodo di conservazione è conforme alla previsione dell'art. 14 del D.L.vo n°24 del 2023 e cioè: i dati sono trattati per il tempo strettamente necessario alla corretta gestione della segnalazione e comunque non oltre 5 anni dalla comunicazione dell'esito finale della procedura di segnalazione. I dati manifestamente non utili alla gestione della segnalazione non sono raccolti o, se inavvertitamente raccolti, sono immediatamente cancellati.

Hanno accesso ai dati:

a) l'Organismo di Vigilanza, individuato dalla società come soggetto gestore delle segnalazioni; è nominato Responsabile del trattamento
b) dipendenti della società a cui l'OdV può chiedere informazioni nel corso della gestione della segnalazione; sono nominati Incaricati del trattamento
c) professionisti esterni alla società a cui l'OdV può chiedere informazioni o consulenze nel corso della gestione della segnalazione; sono nominati Responsabili del trattamento.

I possibili destinatari dei dati sono:

a) pubbliche Autorità competenti.

Le informative rilasciate agli Interessati contengono informazioni in merito ai possibili destinatari ed ai possibili Responsabili del trattamento a cui i dati trattati possono essere trasmessi nel corso del trattamento.

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

La raccolta dei dati è curata dall'OdV nell'ambito dei canali, indicati dalla società, attraverso i quali è possibile eseguire le segnalazioni: canali scritti (mediante invio di raccomandata o e-mail all'OdV) o canali orali (incontro con l'OdV e verbalizzazione dello stesso).

Dopo la raccolta dei dati l'OdV rilascia ricevuta al segnalante ed esegue una prima valutazione della segnalazione, trattando i dati per valutare l'ammissibilità alla segnalazione. In questa fase l'OdV può richiedere al segnalante di integrare la segnalazione con altri dati.

Se la segnalazione è inammissibile, l'OdV procede all'archiviazione della stessa (e quindi dei dati raccolti) e assume un provvedimento motivato.

Se la segnalazione è ammissibile, l'OdV procede all'istruttoria, trattando i dati per valutare la sussistenza dei fatti e delle condotte segnalate e, in ultima analisi, per decidere se la segnalazione è fondata. In questa fase l'OdV può richiedere chiarimenti, informazioni o consulenze al segnalante, ad altre funzioni della società o a professionisti esterni. Quindi in questa fase l'OdV può acquisire altri dati o trasmettere i dati ai citati soggetti per ottenere le delucidazioni necessarie.

Al termine dell'istruttoria, se l'OdV ritiene che la segnalazione sia infondata, l'OdV procede all'archiviazione della stessa (e quindi dei dati raccolti).

Al termine dell'istruttoria, se l'OdV ritiene che la segnalazione sia fondata, l'OdV riferisce in merito all'organo amministrativo della società o alle pubbliche Autorità. I dati sono trattati per illustrare i fatti accertati, le

circostanze a comprova e le cause, nonchè per proporre azioni mitigative o correttive. Dopo ciò la segnalazione ed i dati raccolti sono archiviati a cura dell'OdV.

Le fasi sopra elencate sono regolate altresì dall'atto organizzativo whistleblowing adottato dalla società.

I dati sono conservati per i termini sopra indicati; alla scadenza, l'OdV esegue la distruzione degli stessi.

Le finalità del trattamento sono le seguenti:

a) gestione delle segnalazioni whistleblowing
b) adempimento di obblighi di legge
c) tutela e difesa di diritti in sede stragiudiziale o giudiziale.

Le basi giuridiche del trattamento sono le seguenti:

a) adempimento di obbligo legale (art. 6, co. 1, lett. 'c' GDPR); l'obbligo legale discende dal D.L.vo n°24 del 2023, avendo la società adottato un modello di organizzazione e controllo ai sensi del D.L.vo n°231 del 2001
b) assolvimento di obblighi ed esercizio di diritti in materia di diritto del lavoro (art. 9, co. 2, lett. 'b' GDPR)
c) perseguimento di legittimo interesse del Titolare consistente nella tutela ed esercizio di diritti in sede contenziosa o stragiudiziale (art. 6, co. 1, lett. 'f' GDPR)
d) accertamento, difesa, esercizio di diritti in sede contenziosa (art. 9, co. 2, lett. 'f' GDPR).

In forza di quanto descritto, si può concludere che le attività di trattamento: non contemplano decisioni automatizzate che possono produrre effetti giuridici; non prevedono attività di monitoraggio sistematico o videosorveglianza; non sono eseguite su larga scala (ciò è possibile affermare sulla base delle dimensioni della società e del personale impiegato).

1.2.3. Quali sono le risorse di supporto ai dati?

I trattamenti vengono eseguiti con strumenti informatici e con supporti cartacei, ricorrendo alle seguenti risorse:

a) risorse hardware del Titolare e dell'OdV
b) risorse software del Titolare e dell'OdV
c) archivi cartacei del Titolare e dell'OdV
d) risorse di eventuali Responsabili.

Non è previsto l'utilizzo di nuove tecnologie o soluzioni organizzative innovative.

2 SEZIONE 2: PRINCIPI FONDAMENTALI

Questa sezione permette di generare lo schema di adeguamento secondo i principi di protezione dei dati personali.

Sottosezione 2.1: Proporzionalità e necessità

Questa sezione permette di dimostrare l'implementazione degli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

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

Le finalità del trattamento sono le seguenti:

a) gestione delle segnalazioni whistleblowing

b) adempimento di obblighi di legge
c) tutela e difesa di diritti in sede stragiudiziale o giudiziale.

Le finalità sono esplicitate nelle informative rese agli Interessati.

2.1.2. Quali sono le basi legali che rendono lecito il trattamento?
Le basi giuridiche del trattamento sono le seguenti:

a) adempimento di obbligo legale (art. 6, co. 1, lett. 'c' GDPR)
b) assolvimento di obblighi ed esercizio di diritti in materia di diritto del lavoro (art. 9, co. 2, lett. 'b' GDPR)
c) perseguimento di legittimo interesse del Titolare consistente nella tutela ed esercizio di diritti in sede contenziosa o stragiudiziale (art. 6, co. 1, lett. 'f' GDPR)
d) accertamento, difesa, esercizio di diritti in sede contenziosa (art. 9, co. 2, lett. 'f' 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)?
Sì, l'OdV, nel corso della prima valutazione della segnalazione, valuta se sono stati raccolti dati manifestamente non utili a dare seguito alla segnalazione stessa e, in caso positivo, li cancella immediatamente.
Inoltre, se nel corso della gestione della segnalazione sono inavvertitamente acquisiti (presso il segnalante o nell'ambito delle richieste di informazioni ad altre risorse della società o a professionisti esterni) dati non utili, l'OdV li cancella immediatamente.

2.1.4. I dati sono esatti e aggiornati?

Sì, l'OdV può interloquire con il segnalante o con altri soggetti nel corso della gestione della segnalazione anche allo scopo di controllare l'esattezza o l'aggiornamento dei dati raccolti; l'OdV cancella immediatamente i dati che risultano inesatti o non più aggiornati.

2.1.5. Qual è il periodo di conservazione dei dati?
Il periodo di conservazione è conforme alla previsione dell'art. 14 del D.L.vo n°24 del 2023 e cioè: i dati sono trattati per il tempo strettamente necessario alla corretta gestione della segnalazione e comunque non oltre 5 anni dalla comunicazione dell'esito finale della procedura di segnalazione. I dati manifestamente non utili alla gestione della segnalazione non sono raccolti o, se inavvertitamente raccolti, sono immediatamente cancellati.

Sottosezione 2.2: Misure a tutela dei diritti degli interessati

Questa sezione permette di dimostrare l'implementazione degli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

2.2.1. Come sono informati del trattamento gli interessati?
Viene fornita apposita informativa agli Interessati, ai sensi degli artt. 13 e 14 GDPR.
L'informativa è messa a disposizione degli Interessati sul sito internet della società e viene nuovamente resa all'Interessato al momento del primo contatto con l'OdV nel corso della gestione della segnalazione.
Per esempio, l'OdV allega l'informativa all'atto di confermare al segnalante l'avvenuta ricezione della segnalazione.

2.2.2. Ove applicabile: come si ottiene il consenso degli interessati?
Non è richiesta l'acquizione del consenso per eseguire i trattamenti sopra specificati.

2.2.3. Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?
Gli interessati possono esercitare i propri diritti in qualsiasi momento contattando il Titolare per telefono, a mezzo posta o a mezzo e-mail.
Tuttavia, l'esercizio dei diritti può essere limitato ai sensi dell'art. 2 undecies, co. 1, lett. 'f', del D.L.vo n°196 del 2003 qualora l'esercizio dei diritti in parola possa cagionare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona del segnalante.

2.2.4. Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?
Gli interessati possono esercitare i propri diritti in qualsiasi momento contattando il Titolare per telefono, a mezzo posta o a mezzo e-mail.
Tuttavia, l'esercizio dei diritti può essere limitato ai sensi dell'art. 2 undecies, co. 1, lett. 'f', del D.L.vo n°196 del 2003 qualora l'esercizio dei diritti in parola possa cagionare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona del segnalante.

2.2.5. Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?
Gli interessati possono esercitare i propri diritti in qualsiasi momento contattando il Titolare per telefono, a mezzo posta o a mezzo e-mail.
Tuttavia, l'esercizio dei diritti può essere limitato ai sensi dell'art. 2 undecies, co. 1, lett. 'f', del D.L.vo n°196 del 2003 qualora l'esercizio dei diritti in parola possa cagionare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona del segnalante.

2.2.6. Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?
Sì, l'OdV è formalmente nominato Responsabile del trattamento e gli obblighi in capo al predetto sono enunciati in apposito contratto.

Allo stesso modo, qualora nel corso della gestione della segnalazione l'OdV abbia la necessità di ricorrere a consulenti esterni, è prevista la nomina di questi ultimi a Responsabili del trattamento e la formalizzazione dei relativi obblighi in apposito contratto.

La sottoscrizione del contratto deve sempre precedere la trasmissione dei dati al Responsabile e, quindi, l'inizio del trattamento ad opera del Responsabile.

Nel contratto con il Responsabile sono puntualmente indicate le attività di trattamento delegato ed è specificato il divieto di procedere a trattamenti differenti. Sono inoltre fornite apposite istruzioni di trattamento. Nel contratto, inoltre, sono indicate le risorse che il Responsabile impiega per eseguire il trattamento e sono elencate le misure di sicurezza implementate.

2.2.7. In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?
Non è previsto il trasferimento dei dati fuori dall'UE.

3 SEZIONE 3: RISCHI

Questa sezione permette di valutare i rischi per la riservatezza, alla luce delle misure esistenti o pianificate.

Sottosezione 3.1: misure esistenti o pianificate

Questa sezione permette di indicare le misure (esistenti o pianificate) che contribuiscono alla sicurezza dei dati.

3.1.1. Controllo degli accessi logici

L'accesso alle risorse informatiche dove sono contenuti i dati trattati è possibile solo inserendo le credenziali di autenticazione (username e password) fornite dalla società.
La società fornisce istruzioni per la gestione delle password e, più in generale, per l'utilizzo degli strumenti informatici.
L'OdV garantisce l'adozione di eguali misure presso la propria organizzazione.
Gli strumenti informatici in uso all'OdV non fanno parte del network aziendale: i dipendenti della Società che non abbiano ricevuto un incarico in tal senso non possono accedere ai dati archiviati sugli strumenti informatici dell'OdV..

3.1.2. Tracciabilità

La società ha nominato un amministratore di sistema che gestisce i log di accesso alle risorse informatiche.

3.1.3. Archiviazione

La società utilizza software gestionali che garantiscono la continuità dell'accesso ai dati salvati.
L'OdV garantisce l'adozione di eguali misure presso la propria organizzazione.

3.1.4. Sicurezza dei documenti cartacei

I documenti cartacei sono conservati in armadi chiusi a chiave. La società fornisce istruzioni sulla gestione dei documenti cartacei che, tra l'altro, vietano la copia non autorizzata dei documenti o lo spostamento dei documenti dalla sede di lavoro.
L'OdV garantisce l'adozione di eguali misure presso la propria organizzazione.

3.1.5. Minimizzazione dei dati

L'accesso ai dati è consentito al solo OdV. Altri incaricati possono accedere solo a seguito di apposita valutazione dell'OdV nel corso del processo di gestione della segnalazione e cioè quando si rende necessario acquisire informazioni da altre funzioni aziendali.

3.1.6. Vulnerabilità

Il trattamento dei dati avviene nel contesto di procedure aziendali codificate.
Gli strumenti informatici in uso sono inventariati ed esistono procedure che prescrivono: verifiche sulla genuinità dei software in uso, l'aggiornamento degli stessi, il divieto di uso di software provenienti da fonti non previamente autorizzate dalla società.

3.1.7. Lotta contro il malware

L'accesso alle postazioni informatiche è concesso solo al personale autorizzato, per mezzo delle credenziali fornite dalla società.
La società cura l'istallazione sui dispositivi informatici di antivirus e firewall e adotta procedure sulla gestione di tali applicativi (tra l'altro, è vietata la diattivazione di tali applicativi ed è prescritto il loro costante aggiornamento).
La società fornisce istruzioni per l'utilizzo degli strumenti informatici.
L'OdV garantisce l'adozione di eguali misure presso la propria organizzazione.

3.1.8. Backup

La società adotta procedure per la pianificazione dei back up e per la gestione di eventi di data breach.

L'OdV garantisce l'adozione di eguali misure presso la propria organizzazione.

3.1.9. Manutenzione

La società adotta procedure per scadenziare gli interventi di manutenzione sui dispositivi informatici, appoggiandosi a fornitore esterno (al quale, comunque, non è consentito l'accesso ai dati contenuti nei dispositivi).
I dispositivi informatici non più funzionanti sono avviati allo smaltimento solo dopo avere eseguito la formattazione o aver fisicamente rimosso i dischi rigidi / gli ssd / gli altri formati di memoria dove sono stati memorizzati i dati.
L'OdV garantisce l'adozione di eguali misure presso la propria organizzazione.

3.1.10. Contratto con il responsabile del trattamento

I rapporti con i Responsabili del trattamento sono formalizzati con appositi contratti.
La sottoscrizione del contratto deve sempre precedere la trasmissione dei dati al Responsabile e, quindi, l'inizio del trattamento ad opera del Responsabile.
Nel contratto con il Responsabile sono puntualmente indicate le attività di trattamento delegato ed è specificato il divieto di procedere a trattamenti differenti. Sono inoltre fornite apposite istruzioni di trattamento.
Nel contratto, inoltre, sono indicate le risorse che il Responsabile impiega per eseguire il trattamento e sono elencate le misure di sicurezza implementate.
Nel contratto sono incluse specifiche clausole per garantire agli Interessati di poter sempre esercitare i diritti elencati dal GDPR.
Nel contratto sono incluse specifiche clausole in forza delle quali il Responsabile garantisce assistenza e supporto al Titolare nella gestione di eventi di data breach e nella gestione dei riscontri da fornire a pubbliche Autortità.
Il contratto prevede il diritto del Titolare di procedere alla periodica verifica dell'effettività delle garanzie offerte dal Responsabile.

3.1.11. Sicurezza dei canali informatici

La sicurezza della rete aziendale è garantita dall'adozione di credenziali di accesso e dalla predisposizione di antivirus e firewall.
Sono fornite istruzioni ai dipendenti in merito all'uso ed alla custodia delle credenziali ed al funzionamento di antivirus e firewall (tra l'altro, è esplicitamente vietato in ogni caso la disattivazione di tali presidi).
L'OdV garantisce l'adozione di eguali misure presso la propria organizzazione. Gli strumenti informatici in uso all'OdV sono protetti dall'adozione di credenziali di accesso e dalla predisposizione di antivirus e firewall; essi sono esclusi dal network aziendale e sono inaccessibili dai dipendenti che non abbiano ricevuto incarichi al riguardo.

3.1.12. Controllo degli accessi fisici

L'accesso alla sede aziendale è consentito solo ai dipendenti.
Partners d'affari ed altri visitatori possono entrare solo dopo aver firmato un apposito registro posto nelle vicinanze della porta d'ingresso alla sede aziendale, indicando il motivo della visita.
I visitatori sono subito accompagnati presso le sale riunioni, dove non è conservato alcun tipo di dato personale (nè supporti cartacei o informatici).
La sede aziendale è protetta da antifurto, che viene attivato fuori dagli orari di lavoro.

3.1.13. Tracciabilità

La società ha adottato una procedura per gestire eventi di data breach, nel contesto della quale è prevista l'istituzione di un registro degli incidenti che coinvolgono il corretto trattamento dei dati.
E' previsto lo studio degli incidenti registrati per adottare misure correttive.

L'OdV garantisce l'adozione di eguali misure presso la propria organizzazione e garantisce supporto alla società nella gestione degli eventi di data breach.

3.1.14. Sicurezza dell'hardware

Le procedure aziendali prevedono la periodica esecuzione di back up.
L'OdV garantisce l'adozione di eguali misure presso la propria organizzazione.

3.1.15. Prevenzione delle fonti di rischio

Sono tendenzialmente esclusi trasferimenti di dati al di fuori dell'UE.

3.1.16. Protezione contro fonti di rischio non umane

La sede aziendale è protetta da impianto anti incendio.

Sottosezione 3.2: danni potenziali

Questa sezione permette di indicare i danni specifici potenziali che possono essere identificati per il trattamento che si sta valutando

3.2.1 Danni specifici potenziali

Per il trattamento come sopra descritto, è possibile individuare le seguenti voci di danni potenziali:

a) danno per la reputazione
b) discriminazione
c) furto d'identità e frodi
d) perdite finanziarie
e) danni psicologici
f) perdita del controllo di dati personali
g) perdita di riservatezza di dati personali protetti da segreto professionale
h) impossibilità di esercitare diritti
i) rivelazione non autorizzata di dati relativi al rendimento professionale
j) rivelazione non autorizzata di dati relativi alla situazione economica.

E' possibile ricondurre le voci appena elencate ai seguenti scenari di rischio, in relazione ai quali costituiscono gli impatti potenziali:

Scenari di rischio	Impatti potenziali
A) Accesso illegittimo ai dati	danno per la reputazione; discriminazione; furto d'identità e frodi; danni psicologici; perdita di riservatezza di dati personali protetti da segreto professionale; rivelazione non autorizzata di dati relativi al rendimento professionale; rivelazione non autorizzata di dati relativi alla situazione economica
B) Modifica non autorizzata dei dati	furto d'identità e frodi; perdita del controllo di dati personali; perdita di riservatezza di dati personali protetti da segreto professionale; impossibilità di esercitare diritti
C) Perdita dei dati	perdite finanziarie; danni psicologici; perdita del controllo di dati personali; impossibilità di esercitare diritti

3.2.2 Fonti di rischio e minacce che possono concretizzare gli scenari di rischio

Le fonti di rischio possono essere indicate come segue:

a) fonti umane interne alla società (o all'OdV)
b) fonti umane esterne alla società
c) fonti non umane (eventi atmosferici, incendi, crolli, ecc…)

in quanto si può affermare che gli scenari di rischio sopra elencati possono concretizzarsi a seguito dell'intervento di una delle dette fonti.

Si possono individuare le seguenti minacce (i.e. eventi od azioni delle fonti di rischio) che possono concretizzare gli scenari di rischio:

Scenari di rischio	Minacce
A) Accesso illegittimo ai dati	a) intervento di un dipendente infedele; b) intervento di un terzo (collaboratore esterno, visitatore, ecc…); c) attacco dall'esterno; d) furto di credenziali o strumenti di accesso; e) accesso non autorizzato; f) insufficiente o inefficace formazione
B) Modifica non autorizzata dei dati	a) intervento di un dipendente infedele; b) intervento di un terzo (collaboratore esterno, visitatore, ecc…); c) attacco dall'esterno; d) insufficiente o inefficace formazione
C) Perdita dei dati	a) intervento di un dipendente infedele; b) intervento di un terzo (collaboratore esterno, visitatore, ecc…); c) attacco dall'esterno; d) smarrimento credenziali; e) guasti o problemi tecnici; f) incendi, crolli, ecc…

Sottosezione 3.3: valutazione del rischio

Questa sezione permette di indicare il rischio intrinseco che può interessare il trattamento che si sta valutando ed il rischio residuale (cioè quello che ancora sussiste dopo aver considerato l'influenza delle misure di sicurezza adottate o pianificate

3.3.1. Rischio intrinseco

Definito il rischio come uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità, la valutazione del rischio può essere eseguita tenendo conto della probabilità che l'evento accada e la gravità del danno, o impatto, potenziale che consegue da tale evento.

Associando valori quantitativi ai valori qualitativi di probabilità e gravità, è possibile definire il livello del rischio applicando la formula:

Rischio = Probabilità * Gravità

nonché rappresentare il rischio per mezzo di una matrice come quella seguente:

Livello di gravità dell'evento	4 Massimo	4	8	12	16
	3 Significativo	3	6	9	12
	2 Limitato	2	4	6	8
	1 Trascurabile	1	2	3	4
		1 Trascurabile	2 Limitato	3 Significativo	4 Massimo
		Livello di probabilità dell'evento			

Tanto posto, è possibile definire il livello di rischio dei tre scenari di rischio considerati nella precedente sottosezione. Il livello di probabilità dell'evento può essere quantificato considerando la maggiore o minore concretezza della possibilità che le singole minacce sopra individuate possano verificarsi nella realtà, mentre il livello di gravità dell'evento può essere quantificato considerando l'importanza, globalmente intesa, degli impatti potenziali sopra individuati. Gli esiti dell'operazione appena descritti sono riportati nella seguente tabella:

Scenario di rischio	*Livello di gravità*	*Minaccia*	*Livello di probabilità*	*Livello di rischio*
Accesso illegittimo ai dati	3	intervento di un dipendente infedele	3	9
		intervento di un terzo	2	6
		Attacco dall'esterno	3	9
		furto di credenziali o strumenti di accesso	2	6
		Accesso non autorizzato	3	9
		Insufficiente o inefficiente formazione	2	6
Modifica non autorizzata dei dati	3	intervento di un dipendente infedele	3	9
		intervento di un terzo	2	6
		Attacco dall'esterno	3	9
		Insufficiente o inefficiente formazione	2	6
Perdita dei dati	3	intervento di un dipendente infedele	3	9
		intervento di un terzo	2	6
		Attacco dall'esterno	3	9

		Smarrimento credenziali	2	6
		Guasti o problemi tecnici	2	6
		Incendi, crolli, ecc...	1	3

Il livello di rischio in tal modo definito rappresenta il rischio intrinseco connesso allo scenario di rischio ed alla minaccia presi in considerazione, senza cioè tener conto dell'influenza (specie sul fattore della probabilità dell'evento) delle misure di sicurezza adottate o pianificate.

3.3.2. Rischio residuale

Definito il rischio intrinseco è necessario valutare se le misure di sicurezza sopra elencate (sottosezione 3.1.) possano contribuire a mitigare il rischio e, in caso di risposta positiva, in quale misura. Associando un valore quantitativo al valore qualitativo all'efficacia della misura di sicurezza è possibile definire il livello di rischio residuale, o normalizzato, quale risultato del confronto tra rischio intrinseco e misura di sicurezza applicando la seguente formula:

Rischio (residuale) = Rischio (intrinseco) * Efficacia della m.d.s.

nonché rappresentare il rischio residuale per mezzo di una matrice come quella seguente:

Livello di rischio intrinseco	11-16 Massimo	11-16	8-12	5-6	3-4
	6-10 Significativo	6-10	5-8	3-5	2-3
	3-5 Limitato	3-5	2-4	2-3	1
	1-2 Trascurabile	1-2	1-2	1	0-1
		1 Inadeguata	0,75 Poco adeguata	0,5 Adeguata	0,25 Risolutiva
		Efficacia della misura di sicurezza			

Tanto posto, è possibile definire il livello di rischio residuale degli scenari di rischio e delle minacce più sopra individuate. Il livello di efficacia della misura di sicurezza adottata o pianificata può essere quantificato considerando la pertinenza della stessa alla minaccia da contrastare, nonché l'attitudine a limitare (in modo meno o più apprezzabile) la concretezza della possibilità che la minaccia possa verificarsi; il valore 1 viene assegnato anche nel caso in cui non sia stata adottata o pianificata alcuna misura di sicurezza con riguardo ad una data minaccia.

Gli esiti dell'operazione appena descritti sono riportati nella seguente tabella:

Scenario di rischio e minaccia	*Livello di rischio intrinseco*	*Misure di sicurezza*	*Efficacia delle misure di sicurezza*	*Livello di rischio residuale*
A - a	9	3.1.1; 3.1.2; 3.1.4; 3.1.5	0,5	4,5
A - b	6	3.1.1; 3.1.4; 3.1.5; 3.1.10; 3.1.12	0,5	3
A - c	9	3.1.1; 3.1.4; 3.1.6; 3.1./; 3.1.7; 3.1.8; 3.1.11; 3.1.13; 3.1.15	0,5	4,5
A - d	6	3.1.1; 3.1.2; 3.1.4; 3.1.5; 3.1.11	0,5	3
A - e	9	3.1.1; 3-1.2; 3.1.4; 3.1.5; 3.1.11; 3.1.12	0,25	4,5
A - f	6	3.1.1; 3.1.4; 3.1.6; 3.1.7; 3.1.8; 3.1.9; 3.1.11; 3.1.13; 3.1.14	0,5	3
B - a	9	3.1.1; 3.1.2; 3.1.4; 3.1.5	0,5	4,5
B - b	6	3.1.1; 3.1.4; 3.1.5; 3.1.10; 3.1.12	0,5	3
B - c	9	3.1.1; 3.1.4; 3.1.6; 3.1./; 3.1.7; 3.1.8; 3.1.11; 3.1.13; 3.1.15	0,5	4,5
B - d	6	3.1.1; 3.1.4; 3.1.6; 3.1.7; 3.1.8; 3.1.9; 3.1.11; 3.1.13; 3.1.14	0,5	3
C - a	9	3.1.1; 3.1.2; 3.1.4; 3.1.5	0,5	4,5
C - b	6	3.1.1; 3.1.4; 3.1.5; 3.1.10; 3.1.12	0,5	3
C - c	9	3.1.1; 3.1.4; 3.1.6; 3.1./; 3.1.7; 3.1.8; 3.1.11; 3.1.13; 3.1.15	0,5	4,5
C - d	6	3.1.1; 3.1.3; 3.1.8; 3.1.14	0,5	3
C - e	6	3.1.3; 3.1.8; 3.1.9; 3.1.13; 3.1.14	0,25	3
C - f	3	3.1.16	0,25	1

4 CONCLUSIONI

In esito alle valutazioni eseguite, si può affermare che il trattamento di dati personali in esame può essere eseguito in presenza della completa e costante implementazione delle misure di sicurezza, sia tecniche che organizzative, sopra indicate.
Le misure appena citate, infatti, appaiono tali da mitigare efficacemente il rischio di un non corretto trattamento dei dati personali, attestandolo su un livello limitato.
Le attività di trattamento debbono comunque essere costantemente monitorate dal Titolare del trattamento, allo scopo di garantire un intervento correttivo in tempi rapidi qualora ciò sia reso necessario, tra l'altro, da una modificazione delle caratteristiche del trattamento che implichino l'adozione di nuove o ulteriori misure di sicurezza, oppure dall'evoluzione tecnologica, oppure ancora dalla necessità di implementare nuove e più efficaci modalità di gestione dei dati personali.