Cooperativa Sociale Oasis Soc. Coop.

Valutazione di impatto

ai sensi dell'art. 35, Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016

Indice:

1 Premesse 3

1.1 Il processo di determinazione dell'obbligo di DPIA 4

1.2 I trattamenti soggetti all'obbligo di DPIA 6

1.3 Executive summary 11

2 Metodologia 13

2.1 Contesto 14

2.1.1 Panoramica 14

2.1.2 Responsabilità connesse al trattamento 14

2.1.3 Dati, processi e risorse a supporto 14

2.2 Principi fondamentali 15

2.2.1 Proporzionalità e necessità 15

2.2.2 Misure a tutela dei diritti degli interessati 15

2.3 Rischi 15

2.3.1 Accesso illegittimo ai dati 16

2.3.2 Modifiche indesiderate 17

2.3.3 Perdita di dati 19

2.3.4 Stima dei rischi 20

2.4 Misure di sicurezza 23

2.5 Piano d'azione 25

3 La valutazione d'impatto 25

3.1 Contesto 25

3.1.1 Panoramica del trattamento 25

3.1.2 Responsabilità connesse al trattamento 26

3.1.3 Dati, processi e risorse a supporto 26

3.1.4 Parere del DPO 30

3.2 Principi fondamentali 30

3.2.1 Proporzionalità e necessità 30

3.2.2 Misure a tutela dei diritti degli interessati 32

3.3 Rischi 34

3.4 Misure di sicurezza del Fornitore 41

3.5 Piano d'azione 45

3.6 Conclusioni 46

1 PREMESSE

Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) – di seguito "Regolamento" o "GDPR", acronimo dall'inglese *General Data Protection Regulation*" – ha comportato alcuni importanti cambiamenti nell'approccio di titolari e responsabili del trattamento alla normativa in materia di protezione dei dati personali.

Il GDPR ha introdotto nuovi diritti in capo agli interessati, specifici doveri in capo a coloro che effettuano e determinano il trattamento dei dati personali e ha modificato il modo di rapportarsi con il Garante per la protezione dei dati personali, eliminando diversi casi di interlocuzione obbligatoria preventiva con l'Autorità.

Tra gli adempimenti del tutto nuovi, da leggersi nell'ambito della maggiore responsabilizzazione del Titolare del trattamento, è la Valutazione di impatto sulla protezione dei dati personali (in seguito "DPIA").

La valutazione di impatto sulla protezione dei dati, nota come DPIA, è uno strumento previsto nell'ambito del Regolamento UE per individuare e analizzare i rischi che incombono sulle persone fisiche. Si tratta di uno degli strumenti che sono stati introdotti in sostituzione degli obblighi generali di notifica alle autorità di controllo del trattamento di dati personali previsti dalla direttiva 95/46/CE e che nel tempo si sono rivelati inadeguati a migliorare la protezione dei dati personali.

La DPIA è richiesta al fine di individuare appropriate misure rispetto ai rischi che, a seguito della valutazione di adeguatezza, risultino di particolare magnitudo per i diritti e le libertà delle persone fisiche. Ai sensi dell'articolo 35 del Regolamento UE la valutazione di impatto è prescritta per quei trattamenti, o insiemi di trattamenti, che presentano rischi elevati per gli interessati. Il Regolamento ne prevede espressamente alcuni, integrati ed esplicitati da provvedimenti dell'European Data Protection Board[1] e dall'Autorità Garante privacy nazionale.

Ad avviso del WP29[2], "*Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati,*

[1] In sigla EDPB o in italiano, Comitato europeo per la protezione dei dati, è un organo europeo indipendente, composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati. Ne fanno parte – senza diritti di voto attivi – anche le autorità di controllo sulla protezione dei dati personali degli Stati EFTA/SEE per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati (GDPR). Ha sostituito il Gruppo di Lavoro art. 29 (Working Party art. 29 o WP29).

[2] Il Gruppo è stato istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Oggi sostituito dall'EDPB (European Data Protection Board).

ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). In altre parole, ***una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.***" (documento WP248 rev 01, "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*", adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.

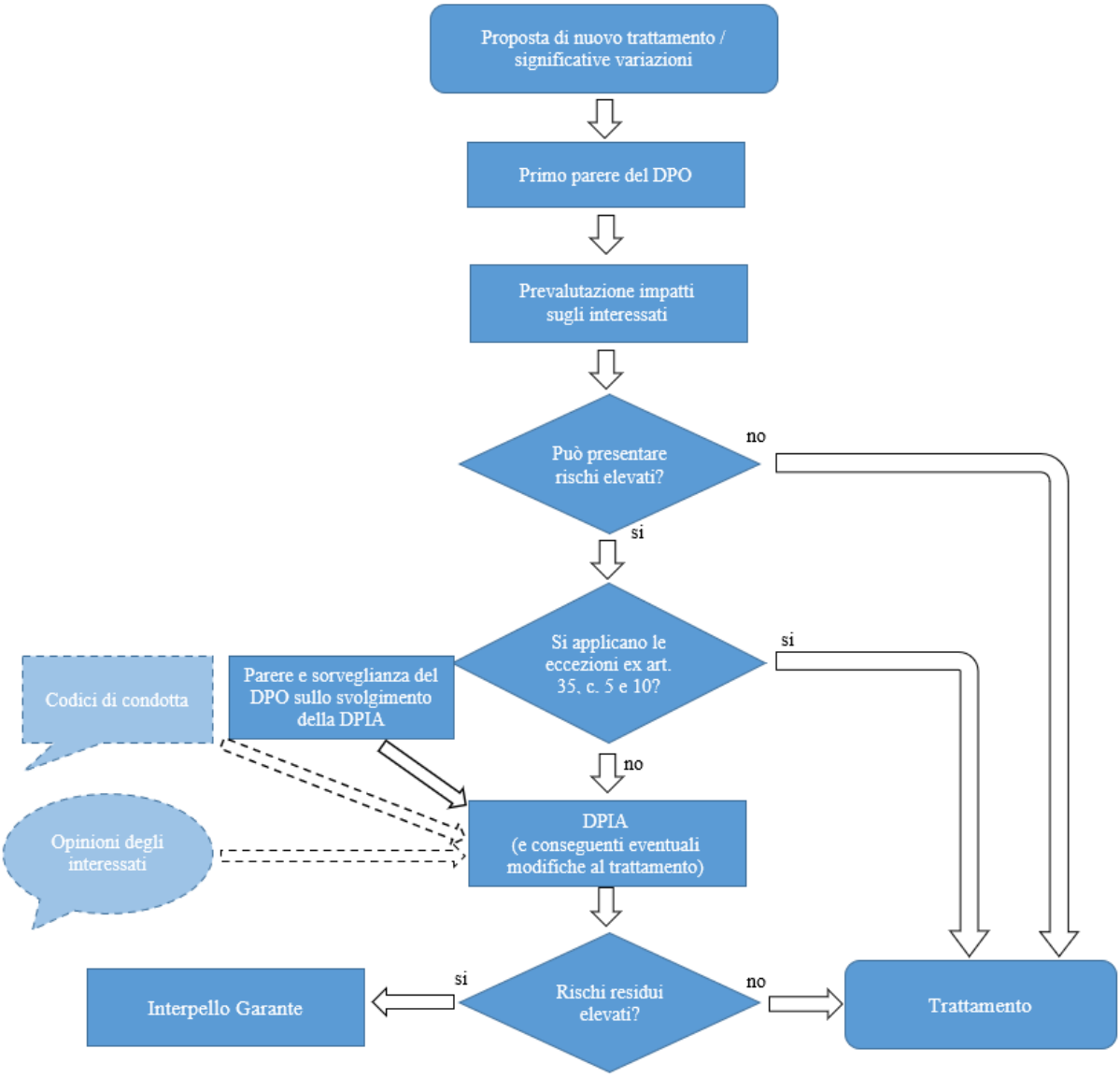
1.1 Il processo di determinazione dell'obbligo di DPIA

Ai sensi dell'articolo 35 del Regolamento, la Valutazione di impatto va eseguita prima di avviare nuovi trattamenti o insiemi di trattamenti che presentano rischi elevati per i diritti e le libertà delle persone fisiche.

Ad avviso del WP29, il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

La Valutazione di impatto va eseguita, nei casi previsti, prima di avviare un nuovo trattamento; l'esecuzione della prevalutazione circa l'applicabilità degli obblighi di cui all'art. 35 deve essere eseguita nelle fasi iniziali del disegno di un nuovo processo dell'ente che richieda il trattamento di dati personali. Gli esiti della DPIA contribuiranno a fornire indicazioni al Titolare utili per il disegno del processo di trattamento e, non da ultimo, a valutare la prosecuzione dello stesso progetto. Lo schema qui riportato illustra i passaggi principali del processo di valutazione di impatto[3].

[3] I riferimenti al DPO nel diagramma di flusso si intendono applicabili nei casi in cui il Titolare abbia effettuato la nomina in quanto tenuto per obbligo imposto dal GDPR, anche in ragione dei provvedimenti dell'EDPB o dell'Autorità Garante per la protezione dei dati personali.



Rispetto allo schema sopra illustrato, il processo di valutazione di impatto può conoscere una significativa differenziazione quantomeno nei seguenti casi:

- trattamenti avviati prima della data di piena applicazione del GDPR che presentano rischi per i diritti e le libertà fondamentali delle persone fisiche: ad avviso del WP29 la Valutazione di impatto è comunque da eseguire, "*nel momento opportuno* […] *nel contesto dei suoi obblighi generali di responsabilizzazione*";
- trattamenti effettuati ai fini dell'adempimento di obblighi di legge: l'art. 35, comma 10, esclude l'applicabilità dell'obbligo di esecuzione di DPIA ai trattamenti effettuati in forza della base giuridica consistente nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto, a condizione, tra l'altro, che "*sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica.*". In mancanza di tale valutazione, il Titolare sarà comunque tenuto ad effettuare la DPIA, escludendo

però già in sede iniziale l'ipotesi di interrompere il trattamento; la DPIA si rivela in quel caso strumento per la valutazione delle misure di sicurezza adottate.

1.2 I trattamenti soggetti all'obbligo di DPIA

L'art. 35, comma 3, prescrive l'obbligo di esecuzione della DPIA per i seguenti casi:

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, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il citato documento WP248 rev 01 aggiunge, in via interpretativa, i seguenti nove criteri, precisando che l'esecuzione della Valutazione di impatto è da ritenersi obbligatoria per i trattamenti che ne soddisfano almeno due:

1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"* (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;

2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che *"hanno effetti giuridici*" o che "*incidono in modo analogo significativamente su dette persone fisiche*" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29;

3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o *"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*" (articolo 35, paragrafo 3, lettera c))[4]. Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

4. dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;

5. trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il

[4] L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29 (cfr. le "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243):
- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.
Il termine "*zona accessibile al pubblico*", a giudizio del WP29, indica qualsiasi luogo aperto a ciascun individuo della popolazione, come ad esempio una piazza, un centro commerciale, una strada, un mercato, una stazione ferroviaria o una biblioteca pubblica.

WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

a) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

b) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

c) la durata, ovvero la persistenza, dell'attività di trattamento;

d) la portata geografica dell'attività di trattamento;

6. creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;

7. dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "*in conformità con il grado di conoscenze tecnologiche raggiunto*" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;

9. quando il trattamento in sé *"impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"* (articolo 22 e

considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

L'Autorità Garante ha dato attuazione a quanto previsto all'art. 35, comma 4 del GDPR ed ha individuato, con proprio provvedimento del 11 ottobre 2018, i seguenti dodici trattamenti da sottoporre a Valutazione di impatto.

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, etc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, etc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248 rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo

a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248 rev. 01.
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Il Decreto Legislativo n. 24 del 10 marzo 2023, recante "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, 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" (di seguito: "**Decreto**") allarga in maniera significativa il perimetro di applicazione della disciplina in materia di whistleblowing (in precedenza limitato alle sole imprese dotate di modello organizzativo, ai sensi del D.lgs. 231/2001) ed introduce le c.d. "segnalazioni esterne".

Il D.Lgs. n. 24/2023 persegue l'obiettivo di rafforzare la tutela giuridica delle persone che segnalano violazioni di disposizioni normative nazionali o europee, che ledono gli interessi e/o l'integrità dell'ente pubblico o privato di appartenenza, e di cui siano venute a conoscenza nello svolgimento dell'attività lavorativa.

Le persone segnalanti beneficiano di protezione a condizione che abbiano avuto fondati motivi di ritenere che le informazioni segnalate fossero vere al momento della segnalazione e che tali informazioni rientrassero nell'ambito di applicazione del Decreto. La tutela e la protezione è estesa a tutti i soggetti collegati in senso ampio all'organizzazione e/o alla persona del segnalante: lavoratori dipendenti pubblici e

privati; lavoratori autonomi; volontari e tirocinanti, retribuiti e non retribuiti; azionisti e membri degli organi di amministrazione, direzione o vigilanza della società.

L'art. 13, comma 6 del Decreto impone al Titolare di eseguire una valutazione di impatto sui processi di trattamento e la protezione dei dati trattati nell'ambito dell'adempimento del Decreto stesso; la fattispecie si aggiunge così alle previsioni introdotte dal WP29 e dall'Autorità Garante per la Protezione dei dati personali.

1.3 Executive summary

In questa sezione sono riportati in sintesi gli elementi fondamentali della presente Valutazione di impatto.

Finalità del trattamento	Whistleblowing
Riferimento alla previsione di obbligo di esecuzione della DPIA, se applicabile	Articolo 13, comma 6, D.lgs. 10 marzo 2023, n. 24
Attività di trattamento eseguita nell'ambito della finalità indicata, sottoposta a Valutazione di impatto	Applicazione delle disposizioni di cui al D.lgs. 10 marzo 2023, n. 24 "*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, 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*"
Parere del DPO	Vista la scelta del Titolare del Trattamento di esternalizzare i canali di raccolta delle segnalazioni e la gestione delle stesse, esaminata la metodologia con cui è stata eseguita la presente valutazione di impatto, considerate le caratteristiche dell'outsourcer, specializzato in materie di compliance con esperienza nella protezione dei dati

		personali e nella gestione delle segnalazioni di cui alla responsabilità amministrativa degli enti ex D.Lgs. 231/2001, considerate le misure di sicurezza indicate nel presente documento, il DPO fornisce parere positivo e concorda sugli esiti della valutazione	
Parere degli interessati		In conformità alla previsione di cui al D.Lgs. 24/2023, sono state sentite le rappresentanze dei lavoratori, che non hanno sollevato obiezioni	
Motivazione della mancata richiesta del parere degli interessati		-	
Basi giuridiche legittimanti il trattamento		Adempimento di un obbligo di legge (art. 6, comma 1., lett. c), GDPR); per quanto concerne i dati particolari e penali potenzialmente raccolti, rispettivamente le previsioni di cui all'art. 9, comma 2, lett. g) e art. 10 GDPR, in combinato disposto con l'art. 2-octies, D.Lgs. 196/2003.	
Periodo di conservazione dei dati		Cinque anni dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto del d.lgs. 10 marzo 2023, n, 24 in materia di Whistleblowing.	
Rischi			
Accesso illegittimo Adozione misure di sicurezza	71,88%	Gravità rischio Probabilità rischio	Importante Limitata
Modifiche indesiderate Adozione misure di sicurezza	90,91%	Gravità rischio Probabilità rischio	Limitata Limitata
Perdita di dati Adozione misure di sicurezza	95,65%	Gravità rischio Probabilità rischio	Limitata Limitata
Necessario piano d'azione / ulteriori misure di sicurezza		Non sono ritenute necessarie ulteriori misure di sicurezza	

2 METODOLOGIA

L'articolo 35 del GDPR definisce, nella sua formulazione, uno standard minimo sulla base del quale articolare la valutazione di impatto. Il punto di partenza dell'analisi è individuato nella redazione di una descrizione sistematica dei trattamenti che presentano i rischi elevati e delle finalità perseguite. Sulla base della descrizione il Titolare è quindi chiamato ad effettuare una valutazione:

- della necessità e proporzionalità dei trattamenti in relazione alle finalità perseguite;
- oltre che dei rischi per i diritti e le libertà degli interessati.

Il Regolamento prevede infine che in essa siano descritte le misure con cui il Titolare del trattamento prevede di 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 GDPR. Tali misure debbono tenere conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. Va sottolineato che il Regolamento non ha definito alcuna specifica istruzione in merito all'output della valutazione, ma ha previsto che l'Autorità Garante debba essere consultata qualora si evidenzi un rischio elevato in assenza di misure atte ad attenuare il rischio. In merito al rischio elevato che porta alla necessità di consultazione preventiva del Garante, il Considerando 84 del GDPR chiarisce che esso è individuabile nei casi in cui il Titolare non possa attenuarlo mediante misure opportune in termini di tecnologia disponibile e costi di attuazione.

Il Titolare del trattamento ha scelto di adottare una metodologia di esecuzione della valutazione di impatto sviluppata recependo alcune tra le principali fonti autorevoli del settore.

In particolare, sono stati considerati:

- la metodologia e lo strumento software sviluppati e proposti dal CNIL (*Commission Nationale de l'Informatique et des Libertés*), ossia l'Autorità di controllo francese in materia di protezione dei dati personali, redatti e condivisi con l'Autorità Garante italiana per la protezione dei dati personali;

- le Linee guida (*Guidelines for SMEs on the security of personal data processing*) ed il Manuale (*Handbook on Security of Personal Data Processing*) pubblicati dall'ENISA, Agenzia europea per la sicurezza delle reti e dell'informazione; i documenti in oggetto sono stati sviluppati in seno all'ENISA con il contributo – tra gli altri – dell'Autorità Garante per la protezione dei dati personali;

- Linea Guida per la Data Protection Impact Assessment, pubblicate dall'Osservatorio Information Security & Privacy del Politecnico di Milano nel febbraio 2018. In particolare, è stato recepito l'elenco della tipologia di minacce, così come esposto nelle seguenti sezioni.

La metodologia proposta dal CNIL ed adottata dal Titolare del trattamento è strutturata nelle seguenti sezioni:

1. **Contesto;**

1.1. **Panoramica del trattamento;**

1.2. **Responsabilità connesse al trattamento;**

1.3. **Dati, processi e risorse a supporto;**

2. **Principi fondamentali;**

2.1. **Proporzionalità e necessità;**

2.2. **Misure a tutela dei diritti degli interessati;**

3. **Rischi;**

3.1. **Accesso illegittimo ai dati;**

3.2. **Modifiche indesiderate dei dati;**

3.3. **Perdita dei dati;**

4. **Misure di sicurezza;**

5. **Piano d'azione.**

Segue l'esposizione degli step metodologici per ogni sezione.

2.1 Contesto

2.1.1 Panoramica

La sezione si apre con l'esposizione, in sintesi, dell'attività svolta dal Titolare del trattamento; successivamente è esposto il contesto del trattamento oggetto di valutazione, le finalità, i risultati attesi, il contesto di utilizzo dei dati, gli eventuali standard applicabili al trattamento.

2.1.2 Responsabilità connesse al trattamento

Sono identificati gli eventuali contitolari del trattamento, i soggetti interni preposti in qualità di persone autorizzate al trattamento nonché gli eventuali outsourcers, in ordine ai quali è esposto anche il dettaglio del trattamento, parte di trattamento o servizio affidatogli.

2.1.3 Dati, processi e risorse a supporto

La sezione definisce e descrive i dettagli del trattamento; sono descritte le categorie degli interessati, la tipologia dei dati trattati, il dettaglio degli stessi dati, suddivisi in specifici campi, ripresi nelle sezioni successive per analizzarne la rispondenza ai principi fondamentali sanciti dal GDPR.

È riportata inoltre l'analisi del ciclo di vita del trattamento – a partire dalle informazioni di analisi della fase di raccolta, i processi di trattamento, l'ambito interno di accessibilità e le eventuali comunicazioni all'esterno dei dati, fino alla fase di sola conservazione o archiviazione e successiva eliminazione e/o anonimizzazione allo spirare del termine temporale indicato.

La sezione è completata dalla descrizione degli asset a supporto del trattamento (informatici, fisici, cartacei).

2.2 Principi fondamentali

2.2.1 Proporzionalità e necessità

Dopo aver descritto le basi giuridiche legittimanti il trattamento, per ogni tipologia di informazione trattata è documentata la rispondenza ai requisiti di adeguatezza, pertinenza e limitazione, nonché alle soluzioni adottate al fine di assicurare l'esattezza e l'aggiornamento dei dati.

2.2.2 Misure a tutela dei diritti degli interessati

Sono esposte le soluzioni adottate per garantire l'esercizio dei diritti degli interessati ed un approfondimento sugli eventuali responsabili del trattamento.

Infine, sono analizzati gli eventuali trasferimenti di dati verso Paesi "terzi", con ciò intendendo Paesi non aderenti allo Spazio Economico Europeo[5].

Come noto, il trasferimento di dati a destinatari posti fuori dallo SEE è legittimo al sussistere dei presupposti prescritti dal Capo V del GDPR. Qualora il trattamento comporti trasferimenti di dati in Paesi terzi, i requisiti di legittimità per il trasferimento sono riportati nella sezione.

2.3 Rischi

Sono analizzati i rischi seguenti:

- accesso illegittimo ai dati;
- modifiche indesiderate;
- perdita di dati.

Per ogni rischio sono individuate le possibili minacce, suddivise per tipologia di fonte (umana interna, umana esterna, non umana. Ove rilevante, la fonte umana è suddivisa tra colposa e dolosa). L'articolazione delle fonti di rischio è inspirata alla metodologia

[5] SEE o Spazio Economico Europeo, alla data di approvazione del presente documento ne fanno parte trenta Paesi: Islanda, Liechtenstein e Norvegia e i 27 stati membri dell'Unione europea.

proposta dal CNIL, gli elenchi delle potenziali minacce è derivante dalle Linee Guida dell'Osservatorio del Politecnico (si veda sezione Metodologia).

In ragione delle differenti minacce e fonti delle minacce, l'analisi per ogni rischio è strutturata secondo le matrici esposte nelle seguenti sottosezioni.

2.3.1 Accesso illegittimo ai dati

Rischio	**Accesso illegittimo ai dati**
Possibili impatti	Effettivo accesso (anche in sola visualizzazione) ai dati trattati dall'azienda da parte di soggetti non aventi diritto al momento della violazione
	Modifiche non autorizzate ai dati
Minacce	
fonte umana interna colposa	dipendente che si rende responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione
fonte umana interna dolosa	vendetta - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per vendetta provocare allarme - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole con la volontà di provocare allarme malevolenza - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per malevolenza lucro - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per possibilità di lucro spionaggio - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un

Rischio	Accesso illegittimo ai dati
fonte umana esterna colposa	tempo a disposizione potenzialmente considerevole per spionaggio
	In accordo con le fonti utilizzate per l'elaborazione della metodologia, si assume che eventuali minacce di fonte umana esterna colposa non possano comportare rischi di accesso illegittimo ai dati
fonte umana esterna dolosa	un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni
fonte non umana	*In accordo con le fonti utilizzate per l'elaborazione della metodologia, si assume che eventuali minacce di fonte non umana non possano comportare rischi di accesso illegittimo ai dati*

2.3.2 Modifiche indesiderate

Rischio	Modifiche indesiderate ai dati
Possibili impatti	comunicazione di informazioni erronee a enti esterni all'azienda (es. istituzioni, società, persone, ecc.)
	comunicazione di informazioni erronee al pubblico (Internet)
	errori nel trattamento o trattamento non conforme
	decisioni errate con effetti sull'Interessato
Minacce	
fonte umana interna colposa	dipendente che si rende responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione

Rischio	Modifiche indesiderate ai dati
fonte umana interna dolosa	vendetta - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per vendetta provocare allarme - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole con la volontà di provocare allarme malevolenza - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per malevolenza lucro - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per possibilità di lucro spionaggio - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per spionaggio
fonte umana esterna colposa	utente/cliente che si rende responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione
fonte umana esterna dolosa	una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni
fonte non umana	*In accordo con le fonti utilizzate per l'elaborazione della metodologia, si assume che eventuali minacce di fonte non umana non possano comportare rischi di modifiche indesiderate ai dati*

2.3.3 Perdita di dati

Rischio	Perdita di dati
Possibili impatti	Impossibilità per l'interessato di fruire dei servizi della Società
	Ritardi significativi nell'erogazione dei servizi
	Indisponibilità di informazioni e servizi per l'interessato
Minacce	
fonte umana interna, colposa o dolosa	eliminazione logica non autorizzata (es. cancellazione dei dati) eliminazione fisica (es. danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei) eliminazione logica o fisica dei dati in formato elettronico, il cui ripristino da documenti cartacei è possibile ma con un impiego di tempo elevato, tale da poter generare effetti sull'Interessato indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (es: perdita di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi) Perdita del supporto fisico di memorizzazione dei dati (es. privazione, sottrazione, smarrimento dei dispositivi contenti i dati oppure dei documenti cartacei)

Rischio	Perdita di dati
fonte umana esterna, colposa o dolosa	eliminazione logica non autorizzata (es. cancellazione dei dati) eliminazione fisica (es. danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei) eliminazione logica o fisica dei dati in formato elettronico, il cui ripristino da documenti cartacei è possibile ma con un impiego di tempo elevato, tale da poter generare effetti sull'Interessato indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (es: sottrazione o sostituzione di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi) Perdita del supporto fisico di memorizzazione dei dati (es. privazione, sottrazione dei dispositivi contenti i dati oppure dei documenti cartacei)
fonte non umana	eliminazione fisica (es. deterioramento dei supporti di memorizzazione o dei documenti cartacei) eliminazione logica o fisica dei dati in formato elettronico (allagamenti, incendi, eventi naturali), il cui ripristino da documenti cartacei è possibile ma con un impiego di tempo elevato, tale da poter generare effetti sull'Interessato indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni a seguito di eventi naturali, incendi, allagamenti (es: perdita di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi) degrado prestazionale dei servizi informatici, che determina l'impossibilità di perfezionare operazioni di trattamento modifiche tecnologiche che rendono impossibile la decodifica di dati rappresentati secondo particolari formati di memorizzazione

2.3.4 Stima dei rischi

Conformemente alla metodologia CNIL, per ogni rischio sono riportate le stime effettuate dal Titolare del trattamento circa la gravità e la probabilità dei rischi.

La gravità del rischio è stimata alla luce degli impatti potenziali e delle misure di sicurezza pianificate o, nei casi in cui il trattamento sia già in essere oppure ne sia prevista l'esecuzione mediante asset già in uso presso il Titolare, delle misure di

sicurezza già adottate. Le misure di sicurezza, censite come indicato alla sezione successiva, sono riportate alla sezione 3.4.

In ordine alla gravità, sono previsti quattro livelli (trascurabile, limitata, importante, massimo) e, per ognuno, tre possibili dimensioni dell'impatto sull'interessato (fisico, materiale, psicologico). Ogni livello è accompagnato da una descrizione e dalla motivazione in base alla quale è stato attribuito.

I valori di rischio sono espressi secondo i parametri e le dimensioni riportate nella seguente matrice.

Gravità rischio	
Trascurabile	Gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente, superabile senza difficoltà
Limitata	Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà
Importante	Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative
Massimo	Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare

Dimensioni dell'impatto		
Trascurabile	**fisico**	es. mal di testa passeggero
	materiale	perdita di tempo dovuta a ripetizione delle procedure o all'attesa della loro effettuazione, riutilizzo dei dati a scopo di pubblicità mirata per beni di consumo corrente ecc.
	psicologico	semplice fastidio, impressione di violazione della privacy senza danno reale (intrusione commerciale) ecc.
Limitato	**fisico**	minore affezione fisica (es: malattia lieve a seguito del mancato rispetto di controindicazioni), diffamazione che dia luogo a rappresaglie fisiche, ecc.
	materiale	pagamenti non pianificati (ad esempio multe non dovute), negazione dell'accesso a servizi amministrativi o commerciali, pubblicità online mirata su un aspetto di vita privata che la persona voleva mantenere riservata ecc.
	psicologico	disturbo psicologico minore ma oggettivo, senso di violazione della privacy senza danni irreparabili, intimidazione sui social network ecc.

Dimensioni dell'impatto		
Importante	**fisico**	grave affezione fisica che provochi danni a lungo termine (aggravamento dello stato di salute a seguito di una errata assunzione di responsabilità o del mancato rispetto di controindicazioni), alterazione dell'integrità fisica, ecc.
	materiale	perdite monetarie non indennizzate, perdita di opportunità uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), perdita dell'abitazione, del posto di lavoro, ecc.
	psicologico	grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc.
Massimo	**fisico**	affezione fisica a lungo termine o permanente, alterazione permanente dell'integrità fisica, decesso
	materiale	rischio finanziario, indebitamento ingente, impossibilità di lavorare, incapacità di ricollocazione, smarrimento di elementi di prova nell'ambito di un contenzioso, perdita di accesso a infrastrutture vitali (acqua, elettricità, ecc.)
	psicologico	disturbo psicologico a lungo termine o permanente, sanzione penale, allontanamento, perdita di legami familiari, perdita della capacità di agire, cambio di stato amministrativo e/o perdita dell'autonomia legale (tutela) ecc.

La probabilità del rischio è stimata alla luce delle minacce, delle fonti di rischio e delle misure pianificate o, nei casi in cui il trattamento sia già in essere oppure ne sia prevista l'esecuzione mediante asset già in uso presso il Titolare, delle misure di sicurezza già adottate. Le misure di sicurezza, censite come indicato alla sezione successiva, sono riportate alla sezione 3.4.

In ordine alla **probabilità**, sono previsti quattro livelli (trascurabile, limitata, importante, massima). Ogni livello è accompagnato da una descrizione e dalla motivazione in base alla quale è stato attribuito.

Probabilità del rischio	
Trascurabile	Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge e codice d'ingresso)
Limitata	Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge
Importante	Appare possibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in uffici dell'organizzazione ove l'accesso è controllato da un incaricato all'ingresso)
Massimo	Appare estremamente facile per le fonti di rischio considerate concretizzare una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione pubblicamente accessibile)

2.4 Misure di sicurezza

La matrice riporta e descrive le misure di sicurezza che prevengono o mitigano i rischi di accesso illegittimo, modifiche indesiderate, perdita dei dati.

L'elenco delle misure è tratto dalla metodologia CNIL; per ogni misura di sicurezza è rilevato lo stato di implementazione (con valorizzazione possibile: si, parzialmente, no, in attuazione, da pianificare), una sintetica descrizione della misura, laddove implementata quantomeno parzialmente e la categoria di rischio che detta misura contribuisce a prevenire.

La matrice delle misure riporta infine le misure astrattamente adottabili in relazione ad ogni tipologia di rischio, in numero assoluto ed in percentuale.

La matrice seguente riporta le misure di sicurezza e l'indicazione della categoria di rischio che la misura può astrattamente contribuire a prevenire.

La colonna "efficacia" indica se la misura contribuisce alla prevenzione delle minacce di Accesso illegittimo (A), Modifica indesiderata (M), Perdita di dati (P).

Misura di sicurezza	Efficacia
crittografia	A, M

Misura di sicurezza	Efficacia
anonimizzazione	A
partizionamento	A
controllo degli accessi logici	A, M, P
Tracciabilità eventi e gestione dei log	M
Politiche di archiviazione / conservazione a norma	A, M, P
Politiche di sicurezza archivi cartacei	A, M, P
Minimizzazione dei dati	A
Politiche di limitazione delle vulnerabilità	A, P
Misure contro i malware	A, P
Sicurezza delle postazioni	A, M, P
Politiche di sicurezza per i siti internet coinvolti	A, M
Politiche di back-up	P
Politiche di manutenzione dispositivi	P
Contratti con i responsabili adeguati	A, M, P
Idonei dispositivi per la sicurezza dei canali informatici	A, M
Controllo degli accessi fisici	A
Rilevazione e tracciatura degli incidenti di sicurezza	M
Sistemi di sicurezza a protezione dell'hardware	A, M, P
Misure per la prevenzione di fonti di rischio	A, M, P
Misure di prevenzione rischi di fonte non umana	P
Funzione con compiti di guida e verifica data protection	A, M, P
DPO nominato ed in carica	A, M, P
Apparato procedurale data protection	A, M, P
Politica dei processi di controllo rischi per i diritti e le libertà degli interessati	A, M, P
Procedure privacy by design	A, M, P
Procedure e gruppo di lavoro definito per data breach	misura esclusivamente mitigativa
Piano di formazione / sensibilizzazione del personale	A, M, P

Misura di sicurezza	Efficacia
Procedura per chiusura accessi lavoratori cessati	A, M, P
Procedura individuazione e gestione terzi che accedono ai dati	A, M, P
Procedura di controlli periodici conformità privacy	A, M, P
Sistemi di cifratura delle comunicazioni	A
Sistemi di pseudonimizzazione	A
Sistemi di analisi, individuazione e rimozione metadati	A
Sistemi di riduzione della sensibilità di dati raccolti	A
Sistemi di riduzione della capacità identificativa	A
Suddivisione dei dati in partizioni indipendenti	A
Restrizioni all'accesso ai dati (need to know)	A, M, P

2.5 Piano d'azione

La sezione descrive il piano d'azione adottato dal Titolare del trattamento per l'adozione delle misure di sicurezza, con la relativa tempistica.

3 LA VALUTAZIONE D'IMPATTO

Le seguenti sezioni riportano le informazioni di analisi del trattamento oggetto di DPIA, in conformità alla metodologia pubblicata dal CNIL.

3.1 Contesto

3.1.1 Panoramica del trattamento

Denominazione del trattamento	Whistleblowing

Finalità	Il trattamento ha la finalità di raccogliere le segnalazioni effettuate ai sensi del D.lgs. 10 marzo 2023, n. 24 ed effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

Risultati attesi	Ricevere e gestire le segnalazioni di cui al D.Lgs. 24/2023 tutelando la riservatezza in primo luogo del segnalante - differenziando in base alla scelta sul consenso al disvelamento dei dati identificativi - nonché delle altre persone fisiche coinvolte

Contesto di utilizzo	Processi di compliance

Standard applicabili	D.Lgs. 24/2023; Linee Guida ANAC Approvate con Delibera n°311 del 12 luglio 2023

3.1.2 Responsabilità connesse al trattamento

Eventuali contitolari	Nessun contitolare

Soggetti interni preposti	Attività esternalizzata; funzioni aziendali competenti per la gestione della segnalazione (che possono trattare i dati identificativi del segnalante solo previo suo espresso consenso)

Responsabili	Reggiani Consulting S.r.l. (in qualità di Responsabile del trattamento per la gestione della segnalazione)

3.1.3 Dati, processi e risorse a supporto

Dati trattati

Categorie di interessati	Segnalanti (soci, amministratori, persone con funzioni di direzione, controllo, vigilanza, rappresentanza, dipendenti o assimilati, collaboratori, liberi professionisti - attuali o che hanno rivestito in passato tali ruoli; candidati alla selezione del personale, dipendenti in periodo di prova); persone fisiche oggetto della segnalazione; potenzialmente: facilitatori

Tipologia di dati trattati	Nome, cognome, dati sull'attività lavorativa, dati di contatto del segnalante (indirizzo postale o email o numero di telefono); ogni altro dato comunicato dal segnalante e riferibile al segnalato, ivi incluse categorie particolari di dati personali e/o dati personali relativi a condanne penale e reati potenzialmente: ogni altro dato comunicato dal segnalante e riferibile al segnalante, ivi incluse categorie particolari di dati personali e/o dati personali relativi a condanne penale e reati.

Dettaglio dati
Nome del segnalante
Cognome del segnalante
Dati sull'attività lavorativa del segnalante
Dati di contatto del segnalante (indirizzo postale o indirizzo e-mail o numero telefonico)
Ogni altro dato personale comunicato dal segnalante e riferibile al segnalato, ivi incluse categorie particolari di dati personali e/o dati personali relativi a condanne penale e reati.
Eventuale: ogni altro dato personale comunicato dal segnalante e riferibile al segnalante, ivi incluse categorie particolari di dati personali e/o dati personali relativi a condanne penale e reati.

Periodo di conservazione	Cinque anni dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto del d.lgs. 10 marzo 2023, n, 24 in materia di Whistleblowing.

Destinatari	Potenzialmente: Studi Legali, Autorità su legittima richiesta

Funzioni interne che possono accedervi	Attività esternalizzata; funzioni aziendali competenti per la gestione della segnalazione (che possono trattare i dati identificativi del segnalante solo previo suo espresso consenso)

Ciclo di vita del trattamento

Descrizione funzionale	Il processo è descritto nella procedura Whistleblowing resa disponibile dalla Società

Modalità di raccolta	Direttamente dal segnalante: la comunicazione può essere effettuata tramite e-mail, tramite il canale vocale registrato o, su richiesta del segnalante, in presenza con un professionista incaricato dal Responsabile.

Fasi del trattamento	Raccolta ed esame della segnalazione; eventuali verifiche, approfondimenti; disposizioni operative, anche disciplinari; feedback al segnalante; eventuali ulteriori azioni per mitigare il rischio di condotte analoghe, possibili azioni in sede contabile, penale, amministrativa, civile

Archiviazione	Archiviazione informatica crittografata, sui sistemi del Responsabile nominato

Conservazione	L'intero processo genera esclusivamente documenti nativi informatici, salvo il raro caso, previsto solo su esplicita richiesta del committente, di previsione ricevibilità di segnalazioni scritte su supporto cartaceo. I documenti sono pertanto conservati in formato informatico, su strutture cloud sicure, ridondate, all'interno del solo Spazio Economico Europeo.

Distruzione / anonimizzazione	Dati cancellati al termine del periodo di archiviazione (5 anni dalla data della comunicazione dell'esito finale della procedura di segnalazione)

Risorse di supporto ai dati

Sistemi operativi	Microsoft Windows server; sistema di instradamento del traffico voce e di registrazione vocale

Server	Server Cloud in uso al Responsabile

Software	Sistema di registrazione vocale del Sub-fornitore; strumenti di office automation

Reti	internet

Uffici	Reggiani Consulting S.r.l. e/o dei sub Responsabili

Strumenti cartacei	Solo stampe provvisorie, trattamento principalmente digitalizzato

3.1.4 Parere del DPO

Parere del DPO	Vista la scelta del Titolare del Trattamento di esternalizzare i canali di raccolta delle segnalazioni e la gestione delle stesse, esaminata la metodologia con cui è stata eseguita la presente valutazione di impatto, considerate le caratteristiche dell'outsourcer, specializzato in materie di compliance con esperienza nella protezione dei dati personali e nella gestione delle segnalazioni di cui alla responsabilità amministrativa degli enti ex D.Lgs. 231/2001, considerate le misure di sicurezza indicate nel presente documento, il DPO fornisce parere positivo e concorda sugli esiti della valutazione

3.2 Principi fondamentali

3.2.1 Proporzionalità e necessità

Scopi del trattamento (specifici, espliciti, legittimi)

Specificità dello scopo	Adempimento degli obblighi di cui al D.lgs. 10 marzo 2023, n. 24

Modalità di esplicitazione delle finalità	Informativa agli interessati

Basi legali che rendono legittimo il trattamento

Basi giuridiche legittimanti	Adempimento di un obbligo di legge (art. 6, comma 1., lett. c), GDPR); per quanto concerne i dati particolari e penali potenzialmente raccolti, rispettivamente le previsioni di cui all'art. 9, comma 2, lett. g) e art. 10 GDPR, in combinato disposto con l'art. 2-octies, D.Lgs. 196/2003.

Adeguatezza, pertinenza e limitazione a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)	
Tipologia dati	**adeguatezza, pertinenza e limitazione**
Nome e cognome	Necessario, il Titolare del trattamento non accetta segnalazioni anonime
data di nascita	Eventuale
condotte attribuite o tenute	necessario per l'istituto del whistleblowing
Professione, incarico, mansioni, dati relativi al lavoro	necessario per l'istituto del whistleblowing
Dati ottenuti da fonte terza a seguito di approfondimenti	necessario per l'istituto del whistleblowing
Potenziali dati particolari	art. 9, comma 2, lett. g)
Potenziali dati relativi a reati o comunque di rilevanza penale	art. 10, in combinato disposto con l'art. 2-octies, D.Lgs. 196/2003

Esattezza ed aggiornamento		
Tipologia dati	**Modalità per garantire esattezza**	**Modalità per garantire aggiornamento**
Nome e cognome	Dati del segnalante raccolti direttamente dall'interessato; dati delle altre persone coinvolte raccolti dal segnalante, da terzi e da altri uffici aziendali	Trattamento puntuale; dati raccolti dal segnalante e poi cristallizzati
data di nascita	Dati del segnalante raccolti direttamente dall'interessato; dati delle altre persone coinvolte raccolti dal segnalante, da terzi e da altri uffici aziendali	Trattamento puntuale; dati raccolti dal segnalante e poi cristallizzati
condotte attribuite o tenute	Dati del segnalante raccolti direttamente dall'interessato; dati delle altre persone coinvolte raccolti dal segnalante, da terzi e da altri uffici aziendali	Trattamento puntuale; verifiche e riscontri, se possibile; altrimenti, contradditorio con il segnalante, in presenza del prescritto consenso

Professione, incarico, mansioni, dati relativi al lavoro	Dati del segnalante raccolti direttamente dall'interessato; dati delle altre persone coinvolte raccolti dal segnalante, da terzi e da altri uffici aziendali	Trattamento puntuale; verifiche e riscontri, se possibile
Dati ottenuti da fonte terza a seguito di approfondimenti	Dati del segnalante raccolti direttamente dall'interessato; dati delle altre persone coinvolte raccolti dal segnalante, da terzi e da altri uffici aziendali	Trattamento puntuale; verifiche e riscontri, se possibile
Potenziali dati particolari	Dati del segnalante raccolti direttamente dall'interessato; dati delle altre persone coinvolte raccolti dal segnalante, da terzi e da altri uffici aziendali	Trattamento puntuale; verifiche e riscontri, se possibile; altrimenti, contradditorio con il segnalante, in presenza del prescritto consenso
Potenziali dati relativi a reati o comunque di rilevanza penale	Dati del segnalante raccolti direttamente dall'interessato; dati delle altre persone coinvolte raccolti dal segnalante, da terzi e da altri uffici aziendali	Trattamento puntuale; verifiche e riscontri, se possibile; altrimenti, contradditorio con il segnalante, in presenza del prescritto consenso

3.2.2 Misure a tutela dei diritti degli interessati

Modalità di rilascio delle informazioni sul trattamento agli interessati	Informativa rilasciata agli interessati alla raccolta dei dati o alla prima occasione utile. Si rinvia al modello di informativa, allegata

Modalità di ottenimento del consenso, se richiesto	Consenso espresso direttamente dall'interessato tramite i canali di segnalazione adottati, come illustrato dall'informativa esposta verbalmente sul canale vocale, in procedura e mediante gli altri strumenti previsti

Modalità di esercizio dei diritti di accesso e di portabilità dei dati da parte degli interessati	Garantiti, senza formalità, per iscritto, tramite i canali indicati; sono previsti limiti, ai sensi dell'articolo 2-undecies, D.Lgs. 196/2003

Modalità di esercizio dei diritti di rettifica e di cancellazione dei dati da parte degli interessati	Garantiti, senza formalità, per iscritto, tramite i canali indicati; sono previsti limiti, ai sensi dell'articolo 2-undecies, D.Lgs. 196/2003

Modalità di esercizio dei diritti di limitazione e di opposizione dei dati da parte degli interessati	Garantiti, senza formalità, per iscritto, tramite i canali indicati; sono previsti limiti, ai sensi dell'articolo 2-undecies, D.Lgs. 196/2003

Responsabili del trattamento e loro obblighi – chiarezza e disciplina contrattuale

	Responsabili
Denominazione	Reggiani Consulting S.r.l.
Ambito di responsabilità	Gestione delle segnalazioni
Eventuali codici di condotta o certificazioni applicabili	Procedure interne di gestione delle segnalazioni, procedure sul trattamento dei dati personali
Accordi formalizzati (data) o da definire (d.d.)	Nomina a Responsabile del trattamento formalizzata contestualmente all'incarico
Elementi a favore considerati per ogni responsabile	Società specializzata nella consulenza in materia di compliance normativa, con particolare focus sulla protezione dei dati personali

Trasferimenti di dati verso Paesi extra SEE[6]

Paesi destinatari dei dati	Valutazione di adeguatezza	Condizione per il trasferimento dei dati
Nessun trasferimento verso Paesi extra SEE	N/A	N/A
Condizione di legittimità trasferimento per ogni Paese	N/A	N/A

[6] Si veda sezione 2.2.2

3.3 Rischi

3.3.1 Accesso illegittimo ai dati

principali impatti sugli interessati se il rischio si dovesse concretizzare	Effettivo accesso (anche in sola visualizzazione) ai dati trattati dall'azienda da parte di soggetti non aventi diritto al momento della violazione, Modifiche non autorizzate ai dati

Principali minacce

Fonte umana interna colposa	
Soggetto agente	minacce
Responsabile del trattamento	dipendente che si rende responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione
Persone autorizzate interne	dipendente che si rende responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione
Persone autorizzate esterne	dipendente che si rende responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione

Fonte umana interna dolosa	
Soggetto agente	minacce
Responsabile del trattamento	provocare allarme - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole con la volontà di provocare allarme
	lucro - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per possibilità di lucro
	spionaggio - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per spionaggio
	provocare allarme - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole con la volontà di provocare allarme

Persone autorizzate interne	malevolenza - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per malevolenza
Persone autorizzate esterne	lucro - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per possibilità di lucro
	vendetta - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per vendetta
	malevolenza - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per malevolenza

Fonte umana esterna	
Soggetto agente	minacce
Attaccante esterno	un attaccante che prende di mira una delle società responsabili del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine
	una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni
Utente / Cliente (interessato)	un attaccante che prende di mira una delle società responsabili del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine

Fonte non umana
Si assume che eventuali minacce di fonte non umana non possano comportare rischi di accesso illegittimo ai dati

Livelli di rischio

Gravità del rischio	
Limitato	
Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative	
Motivazione	Le segnalazioni potrebbero contenere informazioni che attribuiscono condotte gravi, pregiudizievoli per l'immagine e potenzialmente di rilevanza penale, a persone fisiche ignare del contenuto delle stesse. Le condotte potrebbero essere attribuite dal segnalante al segnalato per errore in buona fede o con intento calunnioso o diffamatorio
Impatto fisico	//

Impatto materiale	importante - materiale: perdite monetarie non indennizzate, perdita di opportunità uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), perdita dell'abitazione, del posto di lavoro, ecc.
Impatto psicologico	importante - psicologico: grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc.

Probabilità del rischio	
Limitata	
Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti.	
Motivazione	Gestione con avanzati sistemi di sicurezza; circolazione delle informazioni limitata, con poche persone interne autorizzate (in particolare, per i casi di segnalazione priva di consenso al disvelamento dell'identità del segnalante), seppur anche in tal caso vi è condivisione interna dei dati del segnalato

3.3.2 Modifiche indesiderate dei dati

principali impatti sugli interessati se il rischio si dovesse concretizzare	comunicazione di informazioni erronee a enti esterni all'azienda (es. istituzioni, società, persone, ecc..)
	decisioni errate con effetti sull'Interessato

Principali minacce

Fonte umana interna colposa	
Soggetto agente	minacce
Responsabile del trattamento	dipendente che si rende responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione
Persone autorizzate interne	dipendente che si rende responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione

Fonte umana interna dolosa	
Soggetto agente	minacce

Responsabile del trattamento	lucro - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per possibilità di lucro
	malevolenza - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per malevolenza
Persone autorizzate interne	malevolenza - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per malevolenza
	malevolenza - dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole per malevolenza

Fonte umana esterna colposa	
Soggetto agente	minacce
Utente / Cliente (interessato)	utente/cliente che si rende responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione

Fonte umana esterna dolosa	
Soggetto agente	minacce
Attaccante esterno	un attaccante che prende di mira una delle società responsabili del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine
	una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni

Fonte non umana
Si assume che eventuali minacce di fonte non umana non possano comportare rischi di modifiche indesiderate dei dati

Livelli di rischio

Gravità del rischio	
Limitato	
Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà	
Motivazione	Il processo di accertamento dei fatti è proceduralizzato e prevede, nella sua parte disciplinare o di segnalazione delle autorità, il diritto di difesa dell'incolpato

Impatto fisico	//
Impatto materiale	limitato - materiale: pagamenti non pianificati (ad esempio multe non dovute), negazione dell'accesso a servizi amministrativi o commerciali, pubblicità online mirata su un aspetto di vita privata che la persona voleva mantenere riservata ecc.
Impatto psicologico	limitato - psicologico: disturbo psicologico minore ma oggettivo, senso di violazione della privacy senza danni irreparabili, intimidazione sui social network ecc.

Probabilità del rischio	
Limitata	
Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti.	
Motivazione	Il sistema vede buoni protocolli per l'inalterabilità della segnalazione; il rischio possibile è la segnalazione colposamente o dolosamente inesatta

3.3.3 Perdita dei dati

principali impatti sugli interessati se il rischio si dovesse concretizzare	Indisponibilità di informazioni e servizi per l'interessato

Principali minacce

Fonte umana interna	
Soggetto agente	minacce
Responsabile del trattamento	eliminazione logica non autorizzata (es. cancellazione dei dati)
	eliminazione fisica (es. danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei)
	indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (es: perdita di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi)
Persone autorizzate interne	eliminazione logica non autorizzata (es. cancellazione dei dati)
	eliminazione fisica (es. danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei)
	indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (es: perdita di una chiave di decifratura o di un token

Fonte umana interna	
Soggetto agente	minacce
	hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi)

Fonte umana esterna	
Soggetto agente	minacce
Attaccante esterno	eliminazione logica non autorizzata (es. cancellazione dei dati)
	indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (es: sottrazione o sostituzione di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi)

Fonte non umana	
Soggetto agente	minacce
Incidenti / sinistri / eventi naturali	eliminazione logica non autorizzata (es. deterioramento dei dati)
	eliminazione fisica (es. deterioramento dei supporti di memorizzazione o dei documenti cartacei)
	indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni a seguito di eventi naturali, incendi, allagamenti (es: perdita di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi)

Livelli di rischio

Gravità del rischio	
Limitata	
Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà	
Motivazione	La gestione mediante piattaforma e sistemi informatici ridondati e coperti da back up permetterebbe di qualificare come "trascurabile" il rischio; il superiore livello "limitato" è applicabile alle sole segnalazioni tramite posta cartacea, qualora fossero conservate in originale, non acquisite otticamente. Il rischio è da intendersi per il solo segnalante, che non vedrebbe riscontro alla propria segnalazione
Impatto fisico	//

Impatto materiale	//
Impatto psicologico	limitato - psicologico: disturbo psicologico minore ma oggettivo, senso di violazione della privacy senza danni irreparabili, intimidazione sui social network ecc.

Probabilità del rischio	
Limitata	
Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti.	
Motivazione	La ridondanza delle sale server, l'esecuzione di back up conservati fuori dall'edificio e le altre misure di sicurezza rendono trascurabile la probabilità di perdita di dati

3.4 Misure di sicurezza del Fornitore

Misura di sicurezza	Stato di implementazione	Misura di sicurezza	Accesso illegittimo	Modifiche indesiderate	Perdita di dati
Crittografia	Si	tutti i documenti informatici – sia formati per opera del segnalante, sia creati dagli operatori e professionisti del Responsabile esterno – sono conservati in forma crittografata. è in uso una metodologia di crittografia con chiave simmetrica – standard AES.	X		
Anonimizzazione	No	N/A			
Partizionamento	No	N/A			
controllo degli accessi logici	Si	Ogni utente ha un proprio account. Non esistono account utente comuni.	X	X	X
Tracciabilità eventi e gestione dei log	Si	Sono effettuati log delle attività		X	
Politiche di archiviazione / conservazione a norma	Si	Procedura di archiviazione e conservazione a norma – ove prescritto	X	X	X
Politiche di sicurezza archivi cartacei	Non applicabile	Per la finalità oggetto di DPIA non sono utilizzati supporti cartacei; eventuali documenti cartacei sono acquisiti otticamente ed il cartaceo è immediatamente distrutto	N/A	N/A	N/A
Minimizzazione dei dati	Si	Sono raccolti esclusivamente dati strettamente necessari per la gestione della segnalazione, in conformità al dettato normativo. Il personale è specificamente formato in ordine all'esclusione di dati particolari (dati sensibili), salvo in caso in cui	X		

Misura di sicurezza	Stato di implementazione	Misura di sicurezza	Accesso illegittimo	Modifiche indesiderate	Perdita di dati
		tali informazioni siano assolutamente indispensabili per supportare la segnalazione. Esiste un processo di controllo di secondo livello da parte di figure con responsabilità di coordinamento sulla prima linea di gestione delle segnalazioni; tale processo di controllo può portare alla eliminazione di informazioni eventualmente raccolte fuori dal principio di minimizzazione			
Politiche di limitazione delle vulnerabilità	Si	Sistema antivirus ad aggiornamento automatico, pressoché quotidiano	X		X
Misure contro i malware	Si	Sistemi anti malware installati sui server	X		X
Sicurezza delle postazioni	Si	Misure di sicurezza a protezione delle postazioni e dei dispositivi per gli accessi in mobilità	X	X	X
Politiche di sicurezza per i siti internet coinvolti	Si	cifratura delle comunicazioni dei dati	X	X	
Politiche di back-up	Si	Politiche di back up formalizzate			X
Politiche di manutenzione dispositivi	Si	Manutenzione eseguita			X
Contratti con i responsabili adeguati	Si	Contratto presenti, integrati dalla nomina a responsabile del trattamento	X	X	X
Idonei dispositivi per la sicurezza dei canali informatici	Si	Firewall, rilevatori anti intrusione	X	X	
Controllo degli accessi fisici	Si	Perimetro aziendale controllato e non ci sono aree aperte al pubblico	X		X

Misura di sicurezza	Stato di implementazione	Misura di sicurezza	Accesso illegittimo	Modifiche indesiderate	Perdita di dati
Rilevazione e tracciatura degli incidenti di sicurezza	Si	Procedura data breach		X	
Sistemi di sicurezza a protezione dell'hardware	Si	Misure di sicurezza descritte nella matrice dedicata	X	X	X
Misure per la prevenzione di fonti di rischio	Si	Misure di sicurezza censite in questa sede e nell'analisi del rischio	X	X	X
Misure di prevenzione rischi di fonte non umana	Si	Misure di sicurezza censite in questa sede e nell'analisi del rischio			X
Funzione con compiti di guida e verifica data protection	Si	Modello organizzativo privacy dell’outsourcer	X	X	X
DPO nominato ed in carica	Da aggiornare	DPO nominato e in carica	X	X	X
Apparato procedurale data protection	Si	Procedure formalizzate	X	X	X
Politica dei processi di controllo rischi per i diritti e le libertà degli interessati	Si	Procedure formalizzate	X	X	X
Procedure privacy by design	Si	Procedura formalizzata	X	X	X
Procedure e gruppo di lavoro definito per data breach	Si	Procedura Data Breach		*misura esclusivamente mitigativa*	

Misura di sicurezza	Stato di implementazione	Misura di sicurezza	Accesso illegittimo	Modifiche indesiderate	Perdita di dati
Piano di formazione / sensibilizzazione del personale	Si	Formazione su privacy a tutti; professionisti specializzati	X	X	X
Procedura per chiusura accessi lavoratori cessati	Si	User disattivate al termine del rapporto di lavoro / collaborazione	X	X	X
Procedura individuazione e gestione terzi che accedono ai dati	Si	Accedono ai dati solo soggetti debitamente autorizzati – con nomina a Responsabile o autorizzazione al trattamento – salvo richieste legittime delle Autorità	X	X	X
Procedura di controlli periodici conformità privacy	Si	Procedure Formalizzate	X	X	X
Sistemi di cifratura delle comunicazioni	Si	Comunicazioni cifrate da standard TLS	X		
Sistemi di pseudonimizzazione	No				
Sistemi di analisi, individuazione e rimozione metadati	Non applicabile		N/A		
Sistemi di riduzione della sensibilità di dati raccolti	Non applicabile	I dati sono inseriti solo da persone autorizzate, non direttamente dagli interessati	N/A		
Sistemi di riduzione della capacità identificativa	No				

Misura di sicurezza	Stato di implementazione	Misura di sicurezza	Accesso illegittimo	Modifiche indesiderate	Perdita di dati
Suddivisione dei dati in partizioni indipendenti	No				
Restrizioni all'accesso ai dati (need to know)	Si	Limitazione ai livelli di accesso determinati e appositamente configurati	X	X	X
Misure adottate, quantomeno parzialmente			19	17	19
Percentuale misure adottate			65,63%	81,82%	86,96%

3.5 Piano d'azione

I rischi rilevati rientrano già nelle soglie di accettabilità.

3.6 Conclusioni

Il Titolare:

- Considerato il parere del Responsabile della protezione dei dati personali;
- Tenuto conto del Decreto Legislativo n. 24 del 10 marzo 2023, recante “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, 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”;
- Considerate le Linee Guida ANAC Approvate con Delibera n°311 del 12 luglio 2023;
- Viste le risultanze della Valutazione di impatto;

ritiene non sussistano rischi residui elevati per i diritti e le libertà fondamentali degli interessati e non necessarie ulteriori misure di sicurezza.

Bolzano (BZ), 11/12/2023

il DPO

il legale rappresentante del Titolare