

Sistema Socio Sanitario



**Regione
Lombardia**

**ATS Milano
Città Metropolitana**

ATS MILANO - CITTÀ METROPOLITANA
CORSO ITALIA, 52
MILANO

C.F. - P.IVA 09320520969 09320520969

T. 02/85781
F.02/85782239
W. WWW.ATS-MILANO.IT
PROTOCOLLOGENERALE@PEC.ATS-MILANO.IT

Valutazione d'impatto sulla protezione dei dati

Valutazione d'impatto REGISTRO DEI TUMORI

02/02/2023

Indice

Valutazione d'impatto sulla protezione dei dati	
1 Introduzione	
2 Informazioni essenziali:.....	
3 Pre-assessment	
4 Informazioni sul trattamento	
5 Valutazione proporzionalità in relazione alla finalità.....	
6 Diritti e principi fondamentali	
7 Valutazione del rischio	
7.1 Misure di sicurezza	
Misure di sicurezza sui trattamenti	
Misure di sicurezza sugli applicativi	
Misure di sicurezza sui componenti IT	
Misure di sicurezza sui luoghi fisici	
7.2 Valutazione del rischio	
8 Coinvolgimento delle parti interessate.....	
9 Note.....	

1 Introduzione

Il presente documento “Valutazione d’impatto REGISTRO DEI TUMORI” ha lo scopo di valutare l’impatto sulla protezione dei dati dell’attività di trattamento “REGISTRO DEI TUMORI”, l’impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati ed ha come obiettivo la verifica della protezione dei dati nel software REGISTRO DEI TUMORI.

2 Informazioni essenziali:

Data creazione analisi: 13/12/2021

Data generazione documento: 02/02/2023

Data del prossimo controllo: 01/09/2023

Status: completo

Titolare: ATS MILANO - Città metropolitana

DPO: RPD Interno

Reporter: [***]

3 Pre-assessment

A seguito di una prima analisi, basata sui dodici criteri individuati nell’allegato 1 al provvedimento n. 467 dell’11 ottobre 2018, “Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d’impatto” risulta che nel trattamento preso in esame sono presenti i seguenti criteri:

- **Trattamenti valutativi o di scoring**

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.

- **Dati sensibili o dati di natura estremamente personale**

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 Regolamento UE 2016/679 interconnessi con altri dati personali raccolti per finalità diverse.

- **Trattamento di dati su larga scala**

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).

- **Combinazione o raffronto di insiemi di dati**

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).

- **Dati relativi a interessati vulnerabili**

Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

- **Scambio di dati su larga scala**

Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

Preso atto che il sopracitato documento asserisce che la valutazione d'impatto sulla protezione dei dati debba essere effettuata ogniqualvolta ricorrano almeno un criterio e tenendo conto che nel trattamento preso in esame ne ricorrono 6, il Titolare del trattamento ha ritenuto opportuno procedere all'esecuzione della valutazione d'impatto.

4 Informazioni sul trattamento

ID	Nome	Data creazione	Data ultima modifica
569	REGISTRO DEI TUMORI	13/12/2021	02/02/2023
<p>Il registro tumori dell'ATS di Milano istituito con la DGR n. XI/6818 del 2/8/2022, parte della rete lombarda dei registri tumori, è un sistema attivo di raccolta sistematica di dati personali anagrafici e sanitari dei casi di tumore che insorgono nei residenti nel territorio dell'ATS di Milano, realizzato a fini di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, nonché di elaborazione delle informazioni epidemiologiche e statistiche a supporto delle attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria</p>			



Modalità del trattamento	
cartaceo; informatizzato	
Titolare	
ATS MILANO - Città metropolitana	
Responsabile Protezione dei Dati	
RPD Interno	
Origine dei dati	
Comunicati da terzi - ASST - ENTI PRIVATI ACCREDITATI CON SSL	
Finalità	
Produrre misure dell'incidenza, della sopravvivenza a e della prevalenza dei tumori, Stimare il rischio di malattia per sede e per tipo di tumore, età e genere, Svolgere studi epidemiologici sugli andamenti temporali e la distribuzione territoriale dei casi, sui fattori di rischio e sugli esiti degli interventi diagnostico-terapeutici, Produrre dati anonimi e aggregati per la programmazione, la gestione, il controllo e la valutazione dell'assistenza sanitaria nel contesto degli interventi di prevenzione primaria e secondaria rivolti alle persone e all'ambiente di vita e lavoro, nonché dati riguardanti l'efficacia dei programmi di screening, Monitorare e valutare i dati relativi all'appropriatezza e alla qualità dei servizi diagnostico-terapeutici rivolti ai pazienti affetti da cancro	
Basi giuridiche	
Adempimento di un obbligo legale del Titolare	
Esecuzione di un compito di interesse pubblico	
Riferimenti normativi	

- L. 29/19 relativa alla rete nazionale registri dei tumori , - DGR Lombardia n. XI/6818 del 2/8/2022, - Reg. UE 2016/679: art. 6 c. 1 lettera E, art. 9 c. 2 lettera I, - D. lgs n. 196/03 art. 2 ter; art. 2 sexies c. 2 lettere U, V, CC e DD e c. 3; art. 2 septies c. 5

Categorie di dati	
Personali	Personali identificativi
Particolari	Stato di salute
Categorie di interessati	
Persone fisiche; Utenti del servizio maggiorenni; utenti del servizio minorenni	
Trasferimenti e comunicazione dati	
Regione Lombardia, enti ed istituti di ricerca e società scientifiche previa approvazione del CTS regionale e del comitato etico di riferimento	
Diffusione	
Viene effettuata la diffusione dei dati	
Descrizione dell'attività di diffusione	
In forma esclusivamente aggregata (art. 8 DGR n. XI/6818)	
Profilazione	
Il trattamento comporta attività di profilazione	
Criteri del Gruppo di lavoro Art. 29	
Il trattamento comporta attività di valutazione o assegnazione di un punteggio inclusiva di profilazione e previsione	Si
Il trattamento comporta processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente	No
Il trattamento consiste in un attività di monitoraggio sistematico	No
Il trattamento coinvolge dati sensibili o dati aventi carattere altamente personale	Si

Il trattamento di dati avviene su larga scala	Si
Il trattamento comporta la creazione di corrispondenze o combinazione di insiemi di dati	Si
Il trattamento coinvolge categorie di interessati vulnerabili	Si
Il trattamento coinvolge l'uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	No
Il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	No
Stima del rischio per i diritti e le libertà degli interessati	
Alto	
Pre Assessment	
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.	Si
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).	No

<p>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, ecc. 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, ecc. 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.</p>	<p>No</p>
<p>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 Regolamento UE 2016/679 interconnessi con altri dati personali raccolti per finalità diverse.</p>	<p>Si</p>
<p>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).</p>	<p>Si</p>
<p>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).</p>	<p>Si</p>
<p>Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).</p>	<p>Si</p>

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) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.	No
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).	No
Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.	Si
Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	No
Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	No
Risultato	
DPIA obbligatoria come definito nel provvedimento dell'Autorità garante per la protezione dei dati personali del 2018	
Periodo di conservazione dei dati	
COME DA TITOLARIO REGIONALE	
Descrizione del periodo di conservazione dei dati	
I dati presenti sul sistema informatico del registro tumori devono essere cancellati o resi anonimi in maniera irreversibile trascorso un periodo di 30 anni se digitali o di 10 anni se cartacei dal decesso dell'interessato cui si riferiscono (artt. 6 c. 1 e 6 c. 4 allegato A alla DGR n. XI/6818 del 2/8/2022)	

Allegati	
Dettaglio tecnico vers 1_2.pdf	
DGR n. XI_6818 del 02.08.2022_Registro Tumori.pdf	
informativa_registrotumori_2022.pdf	

Descrizione delle component dedicate al trattamento

Le risorse dedicate al trattamento dei dati costituiscono le componenti che caratterizzano ogni specifico Servizio e la cui analisi determina un'opportuna valutazione degli elementi di rischio in merito agli aspetti di sicurezza, conformità, ecc. Le componenti si distinguono in:

- componenti tecnologiche
 - applicazioni
 - infrastrutture tecnologiche
 - rete
- componenti fisiche
 - asset fisici (documenti cartacei..)
 - sedi fisiche ospitanti dati personali (archivi, sistemi IT, ecc)
- componenti organizzative
 - soggetti interni che supportano l'attuazione del servizio (soggetti IT e non IT)
 - soggetti esterni (fornitore) che supportano l'attuazione (IT e non IT)

Le componenti si possono combinare all'interno di un servizio secondo varie logiche e relazioni. Per quanto riguarda le specifiche componenti, si riportano le seguenti informazioni:

	Componenti organizzative
Soggetti Interni	<i>Descrizione sintetica (es. soggetti facenti parte o meno del personale tecnico informatico, descrizione delle attività svolte in relazione ai trattamenti in esame, formazione ricevuta, procedure che ne disciplinano le mansioni, relazioni con altre componenti)</i>
	Sviluppatore, sistemista, direttore del registro e personale afferente autorizzato

	Componenti tecnologiche
Applicazioni	<i>Descrizione sintetica (es. principali caratteristiche, funzionalità, modalità di autenticazione, relazioni con altre componenti)</i>
	Software registro dei tumori

Infrastrutture IT	<i>Descrizione sintetica (es. principali caratteristiche tecniche e relazioni con altre componenti)</i>
	In cloud aziendale [***]
Rete	<i>Descrizione sintetica (es. tipologia di rete, tecnologie utilizzate, relazioni con altre componenti)</i>
	Infrastruttura [***] accessibile con login [***]

	Componenti fisiche
Risorse ed asset materiali	<i>Descrizione (es. principali caratteristiche, tipologia di asset non latamente inteso come informatico, relazioni con altre componenti)</i>
	Cartelle cliniche cartacee e su CD
Sedi fisiche	<i>Descrizione (es. ubicazione delle sedi anche distaccate o periferiche, principale utilizzo, relazioni con altre componenti)</i>
	[***]

5 Valutazione proporzionalità in relazione alla finalità

Tenuto conto che l'attività di trattamento REGISTRO DEI TUMORI comporta il trattamento delle seguenti categorie di dati personali:

- Personali (Personali identificativi)
- Particolari (Stato di salute)

con riferimento alle seguenti categorie di interessati

- Persone fisiche
- Utenti del servizio maggiorenni
- utenti del servizio minorenni

Il Titolare ritiene che le categorie di dati trattati siano necessari e proporzionali al perseguimento della finalità: Produrre misure dell'incidenza, della sopravvivenza a e della prevalenza dei tumori Stimare il rischio di malattia per sede e per tipo di tumore, età e genere Svolgere studi epidemiologici sugli andamenti temporali e la distribuzione territoriale dei casi, sui fattori di rischio e sugli esiti degli interventi diagnostico-terapeutici Produrre dati anonimi e aggregati per la programmazione, la gestione, il controllo e la valutazione dell'assistenza sanitaria nel contesto degli interventi di prevenzione primaria e secondaria rivolti alle persone e all'ambiente di vita e lavoro, nonché dati riguardanti l'efficacia dei programmi di screening Monitorare e valutare i dati relativi all'appropriatezza e alla qualità dei servizi diagnostico-terapeutici rivolti ai pazienti affetti da cancro

6 Diritti e principi fondamentali

Nel presente capitolo si prendono in considerazione i diritti di accesso, rettifica, cancellazione, portabilità, e opposizione. Lo scopo dell'analisi è evidenziare come ciascuno dei diritti degli interessati rilevi, sia contemplato e lo si pensi implementare nell'attività di trattamento in analisi.

- **Accesso**

Per l'esercizio dei propri diritti l'interessato può rivolgersi:

- Al Titolare (coordinamentourp@ats-milano.it, protocollo generale@pec-ats-milano.it)

- Al Responsabile della protezione dei dati (RPD; privacyRPD@ats-milano.it, protocollo generale@pec-ats-milano.it)

L'interessato ha altresì il diritto di proporre reclamo all'autorità garante per la protezione dei dati personali scrivendo a protocollo@pec.gdpd.it e di presentare ricorso all'autorità giudiziaria

- **Rettifica**

Vedi Accesso

- **Cancellazione**

Vedi Accesso

- **Portabilità**

Vedi Accesso

- **Opposizione**

Vedi Accesso

- **Liceità, Correttezza e Trasparenza**

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato

- **Limitazione della finalità**

I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità

- **Limitazione della conservazione**

I dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati

I dati presenti sul sistema informatico del registro tumori devono essere cancellati o resi anonimi in maniera irreversibile trascorso un periodo di 30 anni se digitali o di 10 anni se cartacei dal decesso dell'interessato cui si riferiscono (artt. 6 c. 1 e 6 c. 4 allegato A alla DGR n. XI/6818 del 2/8/2022)

- **Integrità e riservatezza**

I dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali

Artt. 9, 10 e 11 allegato 1 alla DGR n. XI/6818 del 2/8/2022

- **Limitazione di trattamento**

Vedi Accesso

7 Valutazione del rischio

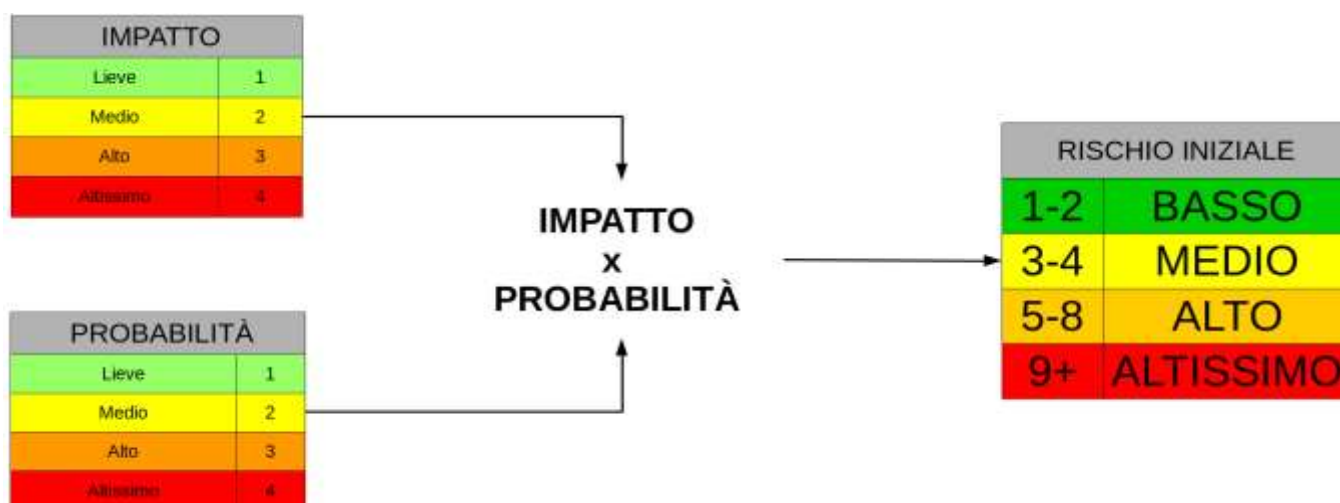
In termini generali la metodologia adottata per la valutazione e gestione del rischio è basata sullo standard ISO31000. Sono state prese in considerazione una serie di ulteriori linee guida e documenti al fine di realizzare una valutazione del rischio calata nel contesto dei rischi per i diritti e le libertà delle persone fisiche con riguardo al trattamento dei loro dati personali.

Nello specifico, gli ulteriori documenti presi in considerazione per effettuare la presente valutazione sono:

- WP29/EDPB – "valutare la particolare probabilità e gravità del rischio";
- CNIL – severity represents the magnitude of a risk;
- Enisa – Handbook on Security of Personal Data Processing
- NIST – Privacy Risk Management for Federal Information Systems;

Al fine di calcolare la magnitudo di un rischio e si adotta una formula del tipo:

$$R_1 = f(M, p)$$



dove:

- **R** : magnitudo del rischio non mitigato
- **M** (Impatto per i diritti e le libertà degli interessati): viene calcolato assegnando un valore su una scala da uno a quattro secondo la seguente scala:

Lieve

Gli interessati non saranno coinvolti o nella peggiore delle ipotesi potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema.



Medio	Gli interessati potrebbero incontrare degli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà
Grave	Gli interessati potrebbero incontrare conseguenze significative, che dovrebbero essere in grado di far fronte seppur con gravi difficoltà
Gravissimo	Gli interessati potrebbero confrontarsi con conseguenze significative o irreversibili.

- **p** probabilità di accadimento del rischio: viene calcolato assegnando un valore su una scala da uno a quattro secondo la seguente scala:

Improbabile	L'avverarsi della minaccia non sembra possibile
Poco Probabile	L'avverarsi della minaccia sembra difficile
Probabile	L'avverarsi della minaccia sembra possibile
Altamente Probabile	L'avverarsi della minaccia sembra probabile

Un controllo di sicurezza può agire sulla probabilità o l'impatto di una Minaccia utilizzate per calcolare il rischio secondo la seguente logica:

$$R_2 = R_1 - (M_n)$$

dove:

- R_2 = rischio finale è il rischio a valle dell'inserimento dei controlli di sicurezza
- R_1 = rischio iniziale come definito nel paragrafo precedente
- M_n = controllo di sicurezza adottato

Allo scopo di rendere quanto più chiara la valutazione dei rischi effettuata in questo capitolo saranno espone in ordine:

1. Le misure di sicurezza adottate divise in tecniche ed organizzative. Le prime sono suddivise su due livelli categoria di misure e tipo di misura e sono correlate all'attività di trattamento presa in esame. Le seconde, anch'esse, divise su due livelli ma correlate agli applicativo o alla natura informatizzata dell'attività di trattamento.
2. Elenco dei rischi con indicazione:
 - Nome della minaccia
 - Fonte della minaccia, che può essere:
 - Umano: soggetto appartenente all'organizzazione del soggetto che effettua la valutazione d'impatto (dipendenti, collaboratori, utenti);
 - Contesto: soggetto esterno all'organizzazione del soggetto che effettua la valutazione d'impatto (concorrenti, agenzie pubbliche, subappaltatori);
 - Strumenti: soggetto non umano (sensori non calibrati, software bug, rottura hardware, disastro naturale);
 - Area d'impatto della minaccia: Disponibilità e/o Integrità e/o riservatezza.
 - Valore dell'impatto e della probabilità. Con possibile motivazione delle scelte.
 - Valore complessivo del rischio non mitigato.
3. Controlli di sicurezza applicati e incidenza di questi su probabilità ed impatto della minaccia. Le misure di sicurezza sono pesate come descritto qui:

https://doc.privacymanager.eu/manuale/valutazione_impatto.html#mitigazione-del-rischio-iniziale-qualitativa



4. Rischio residuo (mitigato).

7.1 Misure di sicurezza**Misure di sicurezza sui trattamenti**

Categoria	Misura
<i>Misure organizzative comuni e generali</i>	Designazione responsabile del trattamento
	Designazione soggetti autorizzati
	Designazione responsabili esterni
	Designazione amministratori di sistema
	Disponibilità e utilizzo informativa ATS
	Raccolta consenso ove previsto
	Registro delle attività di trattamento dei dati personali
	Conoscenza e applicazione modalità esercizio diritti interessato
	Utilizzo modelli Privacy A006 pubblicati in area documentale
	Formazione in materia di protezione dei dati personali
	Applicazione di misure di gestione documentale cartacea
	Applicazione di misure di gestione documentale informatica
	Regolamento interno sull'utilizzo degli strumenti informatici, Internet, PEC e relativi controlli
	Regolamento di Data Breach
<i>Misure di sicurezza fisica</i>	Formazione in materia di prevenzione e protezione
	Sorveglianza sanitaria e attività al video terminale
	Prevenzione e protezione negli ambienti di lavoro
	Gestione delle emergenze incendi e Primo Soccorso con relativo addestramento
	Designazione referenti per la sicurezza
	Accesso consentito solo alle persone autorizzate alle aree ed ai locali
	Videosorveglianza con sistema di allarme
	Sistemi di controllo degli accessi
	Sistemi antincendio
	Sistemi anti allagamento
	Climatizzazione dei locali
<i>Misure tecniche</i>	Procedure di Backup
	Procedura di Disaster Recovery
	Piano di Business Continuity
	Sistema Antivirus
	Sistema Firewall
	Aggiornamenti periodici dei software (es. Sistema Operativo,...)



	Monitoraggio corretto funzionamento e aggiornamento del sistema di protezione
	Procedura gestione password e profili di autorizzazione
	Gestione cartelle di rete e sistemi di Content Management [***]
	Procedura gestione e controllo degli accessi fisici
	Cifratura
	Pseudonimizzazione
	Minimizzazione
	Formazione tecnica specifica
	Procedura MFA - Multifactor Authentication
	SEPARAZIONE

Misure di sicurezza sugli applicativi

Nessuna misura direttamente associata

Misure di sicurezza sui componenti IT

Nessuna misura direttamente associata

Misure di sicurezza sui luoghi fisici

Nessuna misura direttamente associata

7.2 Valutazione del rischio

Categoria: Disponibilità

Minaccia: Distruzione o perdita totale dei dati, per eventi straordinari esterni

Area Impatto: Disponibilità

Fonti di rischio: Contesto, Strumenti

Dettagli minaccia

	Rischio iniziale	Rischio residuo
Impatto	1	1
Probabilità	1	1
Livello di rischio	1	1

Rischio residuo

1 BASSO

Misure di sicurezza

Misure organizzative comuni e generali

Regolamento di Data Breach

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedure di Backup

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Sistema Antivirus

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Sistema Firewall

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Aggiornamenti periodici dei software (es. Sistema Operativo,...)

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Formazione tecnica specifica

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione password e profili di autorizzazione

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Gestione cartelle di rete e sistemi di Content Management [***]

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione e controllo degli accessi fisici

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Sistemi antincendio

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Climatizzazione dei locali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

PSEUDONIMIZZAZIONE

CODIFICA DEI DATI IDENTIFICATIVI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

CIFRATURA

CIFRATURA DATI IN CONSERVAZIONE E NEI CANALI DI TRASMISSIONE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEPARAZIONE

DUE DATABASE DIVERSI PER DATI ANAGRAFICI E DATI SANITARI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

MINIMIZZAZIONE

RACCOLTA SOLO DATI ESSENZIALE PER ATTIVITA' DEL REGISTRO

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEGRETO PROFESSIONALE E/O D'UFFICIO

DOVERE PROFESSIONALE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata



Totale mitigazione del rischio

Mitigazione Impatto	Mitigazione probabilità
100%	100%

Categoria: Disponibilità

Minaccia: Perdita, furto o rimozione non autorizzata di dati personali, anche accidentale

Area Impatto: Disponibilità, Integrità

Fonti di rischio: Umano, Strumenti

Dettagli minaccia

	Rischio iniziale	Rischio residuo
Impatto	1	1
Probabilità	1	1
Livello di rischio	1	1

Rischio residuo

1 BASSO

Misure di sicurezza

Misure organizzative comuni e generali

Regolamento di Data Breach

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedure di Backup

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Sistema Antivirus

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Sistema Firewall

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Aggiornamenti periodici dei software (es. Sistema Operativo,...)

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Formazione tecnica specifica

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione password e profili di autorizzazione

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Gestione cartelle di rete e sistemi di Content Management [***]

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione e controllo degli accessi fisici

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Sistemi antincendio

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Climatizzazione dei locali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

PSEUDONIMIZZAZIONE

CODIFICA DEI DATI IDENTIFICATIVI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

CIFRATURA

CIFRATURA DATI IN CONSERVAZIONE E NEI CANALI DI TRASMISSIONE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEPARAZIONE

DUE DATABASE DIVERSI PER DATI ANAGRAFICI E DATI SANITARI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

MINIMIZZAZIONE

RACCOLTA SOLO DATI ESSENZIALE PER ATTIVITA' DEL REGISTRO

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEGRETO PROFESSIONALE E/O D'UFFICIO

DOVERE PROFESSIONALE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata



Totale mitigazione del rischio

Mitigazione Impatto	Mitigazione probabilità
100%	100%

Categoria: Riservatezza

Minaccia: Accesso non autorizzato ai dati personali, anche accidentale

Area Impatto: Riservatezza

Fonti di rischio: Umano, Strumenti

Dettagli minaccia

	Rischio iniziale	Rischio residuo
Impatto	3	1
Probabilità	2	1
Livello di rischio	6	1

Rischio residuo

1 BASSO

Misure di sicurezza

Misure organizzative comuni e generali

Designazione responsabile del trattamento

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Designazione soggetti autorizzati

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Designazione amministratori di sistema

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Registro delle attività di trattamento dei dati personali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Formazione in materia di protezione dei dati personali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Applicazione di misure di gestione documentale informatica

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Regolamento interno sull'utilizzo degli strumenti informatici, Internet, PEC e relativi controlli

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Regolamento di Data Breach

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Sistema Firewall

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Aggiornamenti periodici dei software (es. Sistema Operativo,...)

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Formazione tecnica specifica

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione password e profili di autorizzazione

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Gestione cartelle di rete e sistemi di Content Management [***]

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione e controllo degli accessi fisici

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Accesso consentito solo alle persone autorizzate alle aree ed ai locali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Videosorveglianza con sistema di allarme

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Sistemi di controllo degli accessi

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

PSEUDONIMIZZAZIONE

CODIFICA DEI DATI IDENTIFICATIVI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

CIFRATURA

CIFRATURA DATI IN CONSERVAZIONE E NEI CANALI DI TRASMISSIONE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEPARAZIONE

DUE DATABASE DIVERSI PER DATI ANAGRAFICI E DATI SANITARI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

MINIMIZZAZIONE

RACCOLTA SOLO DATI ESSENZIALE PER ATTIVITA' DEL REGISTRO

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEGRETO PROFESSIONALE E/O D'UFFICIO

DOVERE PROFESSIONALE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Totale mitigazione del rischio

Mitigazione Impatto	Mitigazione probabilità
100%	100%

Categoria: Riservatezza

Minaccia: Divulgazione non autorizzata dei dati personali, anche accidentale

Area Impatto: Riservatezza

Fonti di rischio: Umano

Dettagli minaccia

	Rischio iniziale	Rischio residuo
Impatto	3	1
Probabilità	2	1
Livello di rischio	6	1

Rischio residuo

1 BASSO

Misure di sicurezza

Misure organizzative comuni e generali

Designazione responsabile del trattamento

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Designazione soggetti autorizzati

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Designazione amministratori di sistema

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Registro delle attività di trattamento dei dati personali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Formazione in materia di protezione dei dati personali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Applicazione di misure di gestione documentale informatica

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Regolamento interno sull'utilizzo degli strumenti informatici, Internet, PEC e relativi controlli

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Regolamento di Data Breach

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Sistema Firewall

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Aggiornamenti periodici dei software (es. Sistema Operativo,...)

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Formazione tecnica specifica

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione password e profili di autorizzazione

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Gestione cartelle di rete e sistemi di Content Management [***]

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione e controllo degli accessi fisici

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Accesso consentito solo alle persone autorizzate alle aree ed ai locali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Videosorveglianza con sistema di allarme

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Sistemi di controllo degli accessi

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

PSEUDONIMIZZAZIONE

CODIFICA DEI DATI IDENTIFICATIVI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

CIFRATURA

CIFRATURA DATI IN CONSERVAZIONE E NEI CANALI DI TRASMISSIONE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEPARAZIONE

DUE DATABASE DIVERSI PER DATI ANAGRAFICI E DATI SANITARI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

MINIMIZZAZIONE

RACCOLTA SOLO DATI ESSENZIALE PER ATTIVITA' DEL REGISTRO

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEGRETO PROFESSIONALE E/O D'UFFICIO

DOVERE PROFESSIONALE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Totale mitigazione del rischio

Mitigazione Impatto	Mitigazione probabilità
100%	100%

Categoria: Riservatezza

Minaccia: Trattamento illecito e/o non conforme alle finalità della raccolta

Area Impatto: Disponibilità, Riservatezza, Integrità

Fonti di rischio: Umano

Dettagli minaccia

	Rischio iniziale	Rischio residuo
Impatto	3	1
Probabilità	2	1
Livello di rischio	6	1

Rischio residuo

1 BASSO

Misure di sicurezza

Misure organizzative comuni e generali

Designazione responsabile del trattamento

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Designazione soggetti autorizzati

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Designazione amministratori di sistema

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Registro delle attività di trattamento dei dati personali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Formazione in materia di protezione dei dati personali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Applicazione di misure di gestione documentale informatica

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Regolamento interno sull'utilizzo degli strumenti informatici, Internet, PEC e relativi controlli

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure organizzative comuni e generali

Regolamento di Data Breach

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Sistema Firewall

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Aggiornamenti periodici dei software (es. Sistema Operativo,...)

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Formazione tecnica specifica

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione password e profili di autorizzazione

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Gestione cartelle di rete e sistemi di Content Management [***]

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione e controllo degli accessi fisici

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Accesso consentito solo alle persone autorizzate alle aree ed ai locali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Videosorveglianza con sistema di allarme

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Sistemi di controllo degli accessi

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

PSEUDONIMIZZAZIONE

CODIFICA DEI DATI IDENTIFICATIVI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

CIFRATURA

CIFRATURA DATI IN CONSERVAZIONE E NEI CANALI DI TRASMISSIONE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEPARAZIONE

DUE DATABASE DIVERSI PER DATI ANAGRAFICI E DATI SANITARI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEGRETO PROFESSIONALE E/O D'UFFICIO

DOVERE PROFESSIONALE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

MINIMIZZAZIONE

RACCOLTA SOLO DATI ESSENZIALE PER ATTIVITA' DEL REGISTRO

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Totale mitigazione del rischio

Mitigazione Impatto	Mitigazione probabilità
100%	100%



Categoria: Integrità

Minaccia: Modifica non autorizzata di dati personali, anche accidentale

Area Impatto: Disponibilità, Riservatezza, Integrità

Fonti di rischio: Umano

Dettagli minaccia

	Rischio iniziale	Rischio residuo
Impatto	1	1
Probabilità	1	1
Livello di rischio	1	1

Rischio residuo

1 BASSO

Misure di sicurezza

Misure organizzative comuni e generali

Regolamento di Data Breach

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Sistema Antivirus

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Sistema Firewall

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Formazione tecnica specifica

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione password e profili di autorizzazione

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Gestione cartelle di rete e sistemi di Content Management [***]

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure tecniche

Procedura gestione e controllo degli accessi fisici

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Accesso consentito solo alle persone autorizzate alle aree ed ai locali

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Videosorveglianza con sistema di allarme

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Misure di sicurezza fisica

Sistemi di controllo degli accessi

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

PSEUDONIMIZZAZIONE

CODIFICA DEI DATI IDENTIFICATIVI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

CIFRATURA

CIFRATURA DATI IN CONSERVAZIONE E NEI CANALI DI TRASMISSIONE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEPARAZIONE

DUE DATABASE DIVERSI PER DATI ANAGRAFICI E DATI SANITARI

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

MINIMIZZAZIONE

RACCOLTA SOLO DATI ESSENZIALE PER ATTIVITA' DEL REGISTRO

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

MISURE SPECIFICHE

SEGRETO PROFESSIONALE E/O D'UFFICIO

DOVERE PROFESSIONALE

Mitigazione Impatto	Mitigazione probabilità
Applicata	Applicata

Totale mitigazione del rischio

Mitigazione Impatto	Mitigazione probabilità
100%	100%

Tabella riassuntiva rischio residuo

Nome	Rischio iniziale		Rischio residuo
Distruzione o perdita totale dei dati, per eventi straordinari esterni	1	→	1
Perdita, furto o rimozione non autorizzata di dati personali, anche accidentale	1	→	1
Accesso non autorizzato ai dati personali, anche accidentale	6	→	1
Divulgazione non autorizzata dei dati personali, anche accidentale	6	→	1
Trattamento illecito e/o non conforme alle finalità della raccolta	6	→	1
Modifica non autorizzata di dati personali, anche accidentale	1	→	1

Esito valutazione d'impatto sulla protezione dei dati

Esito analisi del rischio	
Livello di rischio del trattamento	
BASSO	

8 Coinvolgimento delle parti interessate

- **È stato coinvolto il Responsabile della Protezione dei Dati?**
Il DPO aziendale è stato coinvolto nella stesura della presente valutazione d'impatto

9 Note

Il Titolare del trattamento