VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

GDPR Regolamento UE 2016/679

AZIENDA/ORGANIZZAZIONE:

Società italiana di neurologia

LEGALE RAPPRESENTANTE:

Presidente SIN

SEDE LEGALE: Via del Rastrello, 7 — 53100 Siena.

MAIL: info@neuro.it

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 paragrafo 3 del Regolamento 2016/679).

OBBLIGO DPIA
Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione si rende necessaria nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

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

CRITERI DA CONSIDERARE PER OBBLIGO DPIA
Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE
Secondo le buone prassi, la valutazione d'impatto sulla protezione dei (DPIA) dati viene riesaminata continuamente e rivalutata con regolarità periodica.

ALGORITMO VALUTAZIONE

1° STEP: IDENTIFICAZIONE DEI TRATTAMENTI

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (analogica, digitale, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze di tale evento (C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla probabilità di accadimento dell'evento P è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	Molto Probabile
5	Quasi certo

Alle conseguenze (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di probabilità e conseguenze è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	$(1 \leq LR \leq 3)$
Medio - basso	$(4 \leq LR \leq 6)$
Rilevante	$(8 \leq LR \leq 12)$
Alto	$(15 \leq LR \leq 25)$

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA**:**

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala

6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3° STEP: DPIA – valutazione del rischio normalizzato

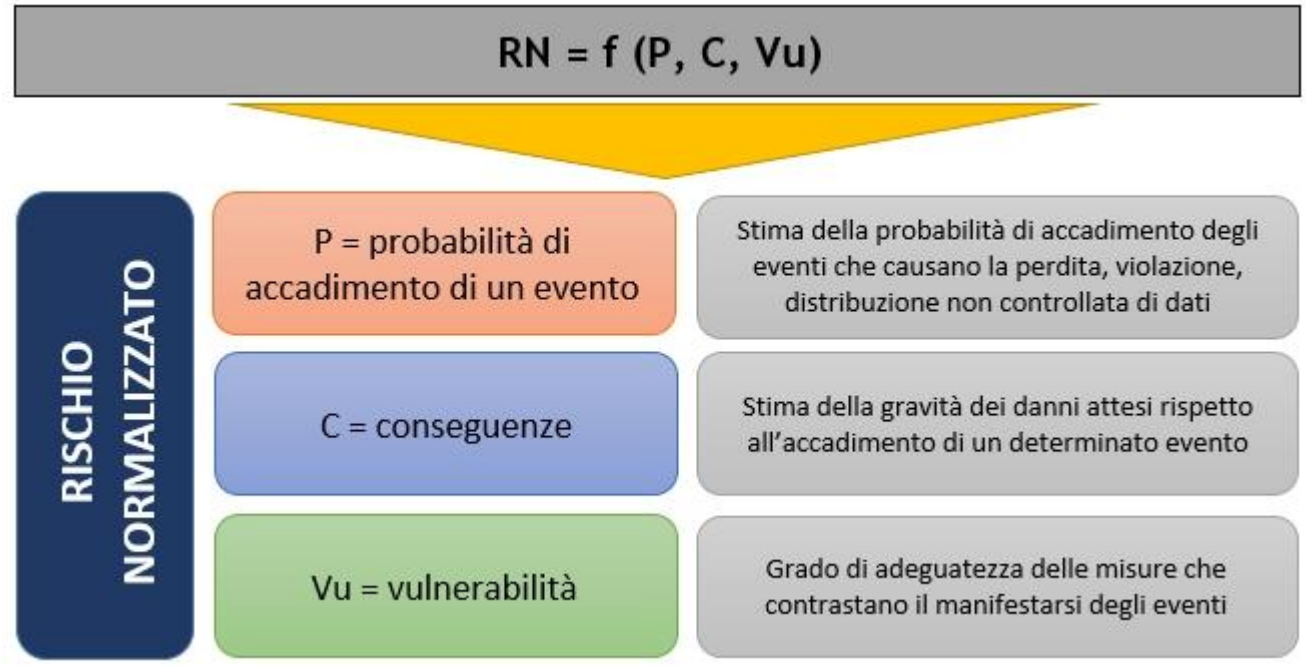
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range **15 ÷ 25**, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.
La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, Vu)

Dove:

P = probabilità
C = conseguenze generate dall'evento
V = vulnerabilità rispetto al grado di adeguatezza delle misure



In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla probabilità P è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle conseguenze (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Rispetto al 1° STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

PROBABILITÀ					
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	$(1 \leq Ri \leq 2)$
Basso	$(3 \leq Ri \leq 4)$
Rilevante	$(6 \leq Ri \leq 9)$
Alto	$(12 \leq Ri \leq 16)$

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.
Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	• **Perdita** • **Distruzione non autorizzata**
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• **Perdita** • **Distruzione non autorizzata**
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione corrente, interruzione collegamenti di rete, ecc.)	• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata** • **Divulgazione non autorizzata** • **Accesso dati non autorizzato**
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata** • **Divulgazione non autorizzata** • **Accesso dati non autorizzato**
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata** • **Divulgazione non autorizzata** • **Accesso dati non autorizzato**
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata** • **Divulgazione non autorizzata** • **Accesso dati non autorizzato**

Per ricavare il Rischio Normalizzato **RN**, viene introdotto il fattore **Vulnerabilità Vu che** fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla Vulnerabilità (**Vu**) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	**Adeguate**	**0,25**
2	**Parzialmente adeguate**	**0,5**
3	**Inadeguate**	**1**

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- **0,25;**
- **0,5;**
- **1.**

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il

valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	**1**	**$1 < RN \leq 2$**	**$3 \leq RN \leq 4$**	**$6 \leq RN \leq 9$**	**$12 \leq RN \leq 16$**
	0,5	**$0,5 < RN \leq 1$**	**$1,5 \leq RN \leq 2$**	**$3 < RN \leq 5$**	**$6 \leq RN \leq 8$**
	0,25	**$0,25 \leq RN \leq 0,5$**	**$0,75 \leq RN \leq 1$**	**$1,5 \leq RN < 3$**	**$3 \leq RN \leq 4$**
		$1 \leq Ri \leq 2$	**$3 \leq Ri \leq 4$**	**$6 \leq Ri \leq 9$**	**$12 \leq Ri \leq 16$**
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	**Valori di riferimento**
Molto basso	**$0,25 \leq RN \leq 1$**
Basso	**$1 < RN < 3$**
Rilevante	**$3 \leq RN \leq 9$**
Alto	**$12 \leq RN \leq 16$**

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia ALTA, il Titolare attiva l'iter di consultazione del Garante.

INQUADRAMENTO

La SIN è stata fondata nel 1907 ed ha lo scopo istituzionale di promuovere in Italia gli studi neurologici, finalizzati allo sviluppo della ricerca scientifica, alla formazione, all'aggiornamento degli specialisti, e al miglioramento della qualità professionale nell'assistenza ai soggetti con malattie del sistema nervoso.

La SIN è composta da un Ufficio di Presidenza e da un Consiglio Direttivo, così come meglio illustrato nell'organigramma allegato al presente Manuale e sul Sito Istituzionale.

La sede della SIN è, da Statuto, presso la Segreteria Organizzativa (SienaCongress) Via del Rastrello, 7 — 53100 Siena.

La SIN dispone di una Segreteria Organizzativa, Siena Congress, e di una Segreteria Tecnica, Asti Incentives & Congressi srl.

La SIN ha inoltre istituito diverse Sezioni Regionali e Interregionali (che coprono territorialmente tutta la Nazione) nate per promuovere un ampio scambio di informazioni tra i settori speculativi ed applicativi della Neurologia. Le Sezioni Regionali e Interregionali hanno una propria Assemblea ed un Segretario, coadiuvato da un Collegio di Segreteria, la cui attività è disciplinata da apposito regolamento.

L'iscrizione alla Società Italiana di Neurologia è riservata ai medici specialisti o specializzandi in neurologia; per neurologi specializzandi si intende riferirsi a coloro che sono ancora iscritti ad una scuola di specializzazione o si sono diplomati negli ultimi due anni dalla data di presentazione della domanda di iscrizione alla SIN. Ai neurologi specializzandi, la SIN, offre la possibilità di iscriversi usufruendo della quota ridotta, che sarà applicata fino alla decadenza dei requisiti.

Il numero dei soci si è stabilizzato negli ultimi anni, raggiungendo nel 2017 il numero di 2396.

La SIN, tramite la "Fondazione Società Italiana di Neurologia (fondata il 12 aprile 2017 e riconosciuta dalla Prefettura di Siena a settembre 2017), progetta e organizza numerosi Eventi formativi (Congressi, Convegni e Riunioni regionali) la cui frequenza da diritto ai crediti della Educazione Medica Continua (ECM).

Tra le principali iniziative SIN possiamo citare il Congresso annuale, che rappresenta oramai l'appuntamento annuale più importante di confronto scientifico e di aggiornamento professionale per i neurologi italiani e per la cui iscrizione i soci SIN hanno importanti agevolazioni.

Il Congresso è diviso in diverse parti, alcune delle quali destinate alla libera comunicazione dei risultati conseguiti dai gruppi di ricerca, altre dedicate all'aggiornamento su specifici temi, decisi di anno in anno dal Consiglio Direttivo.

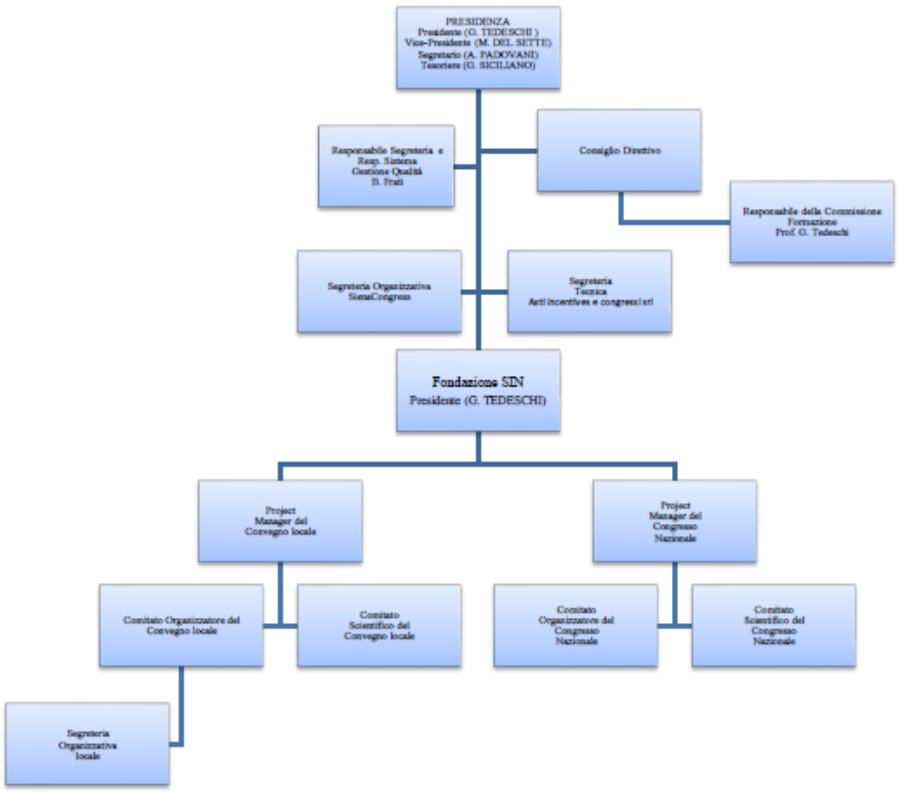
La frequenza al Congresso da diritto ai crediti della Educazione Medica Continua, che vengono divisi nei singoli eventi Congressuali, in maniera tale che ognuno liberamente scelga quali sessioni frequentare.

Particolare attenzione è da sempre dedicata ai giovani neurologi, che hanno a disposizione numerose borse per frequentare gratuitamente il Congresso. I gruppi di Studio e Associazioni autonome aderenti alla SIN, che sono oramai giunti al ragguardevole numero di 35, hanno spazi riservati al Congresso, con lo scopo di informare i neurologi sugli avanzamenti negli specifici settori dei quali si occupano.

Inoltre la SIN, sempre nel 2017, ha istituito un Centro Studi che non è figura giuridica autonoma ma che ha comunque un proprio "board" composto da un Coordinatore, tre collaboratori scientifici un Segretario Scientifico e una Segretaria Organizzativa. Obiettivi del Centro Studi sono i seguenti: 1. Linee Guida, 2. Rete di Centri Collaborativi e Epidemiologia, 3. Biblioteca, 4. Censimento attività di ricerca neurologica in Italia, 5. Censimento Strutture Neurologiche.

La SIN ha una rivista ufficiale, il Neurological Sciences, che ha raggiunto nel 2005 un Impact Factor superiore all'1, e che la colloca, quindi, fra le riviste più importanti d'Europa.

Sin	MANUALE DELLA QUALITA'	All. 1 Sez. 05
	Organigramma Nominativo	



13/10/2019

PARTI INTERESSATE
Clienti (sponsor)
Soci

Clienti (utenti dei corsi di formazione)
Presidenza
Personale della Segreteria organizzativa
Fornitori
Enti territoriali (Città metropolitana, Regione, Stato)
Gruppi di pressione (associazioni di malati)
Competitors
Segreteria Organizzativa

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA

- Gestione del personale
- Gestione partner e approvvigionamento
- Progettazione e sviluppo dei servizi
- Organizzazione ed erogazione di eventi nell'area delle neuroscienze cliniche

Gestione del personale

Politica aziendale che riguarda la gestione del personale in merito a: assunzione, attività formative, valutazioni, pagamenti, oneri contributivi assicurativi, previdenza sociale ecc. Presenza di un MOG ex D.Lgs 231-01 e di un codice etico.

Gestione dei Partner e dell'approvvigionamento

Politica aziendale che riguarda la gestione degli stakeholder e dei fornitori in merito a: dati di identificazione, dati per trasferimenti finanziari, ex art. 9 Regolamento UE 2016/679. Presenza di un MOG ex D.Lgs 231-01 e di un codice etico.

Progettazione e sviluppo dei servizi /Organizzazione ed erogazione di eventi nell'area delle neuroscienze cliniche

Gestione di dati personali, identificativi e non sensibili (in particolare, nome, cognome, codice fiscale, p. iva, email, numero telefonico – in seguito, "dati personali" o anche "dati") comunicati in fase di registrazione al sito web del Titolare e/o all'atto dell'iscrizione ai servizi offerti dal medesimo portale e dal Titolare. Dati di identificazione dei partner, clienti e dei Soci, dati per trasferimenti finanziari. Presenza di un MOG ex D.Lgs 231-01 e di un codice etico. Solo previo specifico e distinto consenso (artt. 23 e 130 Codice Privacy e art. 7 GDPR), per finalità di marketing dei servizi associativi e informative connesse alla vita associativa previsto invio via email di newsletter, comunicazioni e/o materiale informativo su prodotti o servizi offerti dal Titolare.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	**Adeguate**
Impianto elettrico dotato di misure salvavita atte anche ed evitare cortocircuiti e possibili incendi.	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	**Adeguate**
L'impianto elettrico è certificato ed a norma.	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	**Adeguate**
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati digitali e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	**Adeguate**
Sono definiti i ruoli e le	• Azioni non autorizzate (Errori	**Adeguate**

responsabilità.	volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	**Adeguate**
Sono utilizzati software antivirus e anti intrusione.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	**Adeguate**
Viene eseguita opportuna manutenzione.	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	**Adeguate**
È stato fatto il piano di emergenza	• Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	**Adeguate**

VALUTAZIONE DEI RISCHI (DPIA)

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• **Perdita** • **Distruzione non autorizzata**		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Improbabile	**Limitate**	**Basso**
VALUTAZIONE RISCHIO NORMALIZZATO ***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi***		
Rischio intrinseco - Ri	**Vulnerabilità – Vu**	**Rischio normalizzato - RN**
Basso	**0,25**	**Molto basso**

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata** • **Divulgazione non autorizzata** • **Accesso dati non autorizzato**		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Improbabile	**Limitate**	**Basso**
VALUTAZIONE RISCHIO NORMALIZZATO ***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi***		
Rischio intrinseco - Ri	**Vulnerabilità – Vu**	**Rischio normalizzato - RN**
Basso	**0,25**	**Molto basso**

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata** • **Divulgazione non autorizzata** • **Accesso dati non autorizzato**		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Improbabile	**Limitate**	**Basso**
VALUTAZIONE RISCHIO NORMALIZZATO ***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi***		
Rischio intrinseco - Ri	**Vulnerabilità – Vu**	**Rischio normalizzato - RN**
Basso	**0,25**	**Molto basso**

PERICOLO
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
RISCHI
• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata** • **Divulgazione non autorizzata** • **Accesso dati non autorizzato**

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	**Marginali**	**Basso**
VALUTAZIONE RISCHIO NORMALIZZATO ***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi***		
Rischio intrinseco - Ri	**Vulnerabilità – Vu**	**Rischio normalizzato - RN**
Basso	**0,25**	**Molto basso**

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata**		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	**Limitate**	**Rilevante**
VALUTAZIONE RISCHIO NORMALIZZATO ***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi***		
Rischio intrinseco - Ri	**Vulnerabilità – Vu**	**Rischio normalizzato - RN**
Rilevante	**0,5**	**Rilevante**

A valle della DPIA l'attività risulta a rischio **Rilevante**