|  |
| --- |
|  |
|  |  |  |
|  |
| **VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI***ai sensi del GDPR 2016/679 e normativa nazionale in vigore* |
| **Organizzazione** | **Direzione Didattica "San Giovanni" - Terni**  |
|  |
|

|  |  |
| --- | --- |
| TITOLARE | Fiorillo Teresa Assunta |

|  |  |
| --- | --- |
| SEDE | Sede CentraleVia Liutprando 32, 05100Terni - TR |

 |
| Data revisione: 07/01/2019 |
|  |

# 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 del Regolamento 2016/679).

# OBBLIGO DPIA

Ai sensi dell’articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

1. 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;
2. 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;
3. 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 dati viene riesaminata continuamente e rivalutata con regolarità.

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 (cartacea, elettronica, 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 X 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 | M. 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 *≤ LR ≤* 3*)* |
| Medio - basso | *(*4 *≤ LR ≤* 6*)* |
| Rilevante | *(*8 *≤ LR ≤* 12*)* |
| Alto | *(*15 *≤ LR ≤* 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 *≤ Ri ≤* 2*)* |
| Basso | *(*3 *≤ Ri ≤* 4*)* |
| Rilevante | *(*6 *≤ Ri ≤* 9*)* |
| Alto | *(*12 *≤ Ri ≤* 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 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 ≤* 2 | 3 *≤ RN ≤* 4 | 6 *≤ RN ≤* 9 | 12 *≤ RN ≤* 16 |
| 0,5 | 0,5 *< RN ≤ 1* | 1,5 *≤ RN ≤* 2 | 3 *< RN ≤* 5 | 6 *≤ RN ≤* 8 |
| 0,25 | 0,25 *≤ RN ≤* 0,5 | 0,75 *≤ RN ≤* 1 | 1,5 *≤ RN <* 3 | 3 *≤ RN ≤* 4 |
|  |  | 1 *≤ Ri ≤* 2 | 3 *≤ Ri ≤* 4 | 6 *≤ Ri ≤* 9 | 12 *≤ Ri ≤* 16 |
|  |  | Ri |

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

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

# 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

* Scuole ed Università

## Scuole ed Università

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Struttura |

|  |  |
| --- | --- |
|  | Sede legale |
|  | Sede amministrativa |
|  | Sede operativa |

 |

|  |
| --- |
| Personale coinvolto |
| Titolare del trattamento | Fiorillo Teresa Assunta |
| Persone autorizzate |

|  |
| --- |
| Fiorillo Teresa Assunta, c.f. FRLTSS67D41G190C* Blocco
* Cancellazione
* Comunicazione
* Conservazione
* Consultazione
* Diffusione
* Distribuzione
* Elaborazione
* Interconnessione
* Modifica
* Organizzazione
* Raccolta
* Raffronto
 |
| Satta Mirella, c.f. STTMLL61L64B354Z* Blocco
* Cancellazione
* Comunicazione
* Conservazione
* Consultazione
* Diffusione
* Distribuzione
* Elaborazione
* Interconnessione
* Modifica
* Organizzazione
* Raccolta
* Raffronto
 |
| Salvati Angela, c.f. SLVNGL64C47L117Q* Blocco
* Cancellazione
* Comunicazione
* Conservazione
* Consultazione
* Distribuzione
* Elaborazione
* Interconnessione
* Modifica
* Organizzazione
* Raccolta
 |
| Colantoni Anna Teresa, c.f. CLNNTR61H45L117D* Blocco
* Cancellazione
* Comunicazione
* Conservazione
* Consultazione
* Distribuzione
* Elaborazione
* Interconnessione
* Modifica
* Organizzazione
* Raccolta
 |
| Daminato Carla, c.f. DMNCRL58M48L117V* Blocco
* Cancellazione
* Comunicazione
* Conservazione
* Consultazione
* Distribuzione
* Elaborazione
* Interconnessione
* Modifica
* Organizzazione
* Raccolta
 |
| Comella Roberto, c.f. CMLRRT63C03L117U* Blocco
* Cancellazione
* Comunicazione
* Conservazione
* Consultazione
* Distribuzione
* Elaborazione
* Interconnessione
* Modifica
* Organizzazione
* Raccolta
 |

 |
| Partners - Responsabili esterni |

|  |
| --- |
| Bossi Angelo, c.f. BSSNGL50D13D745E * Consultazione
* Elaborazione

Madisoft s.p.a, p.iva 01818840439* Conservazione
* Consultazione
* Modifica
* Elaborazione
* Raccolta

SosPrivacy.net di Bruschi Anna Rita, p.iva 03624640540* Consultazione
* Elaborazione
 |

 |
| Altro |  |

|  |
| --- |
| Processo di trattamento |
| Descrizione |

|  |
| --- |
| Trattamento di dati personali di Dipendenti, Docenti, Ricercatori, Dirigenti, Tecnici, Amministrativi e Studenti |

 |
| Fonte dei dati personali |

|  |
| --- |
| Forniti da terzi |
| Raccolti direttamente |

 |
| Base giuridica per il trattamento per dati comuni (art. 6 GDPR) |

|  |
| --- |
| Consenso |
| Contratto |
| Legge |

 |
| Base giuridica per il trattamento per dati particolari (art. 9 GDPR) |

|  |
| --- |
| Consenso |
| Contratto |
| Legge |

 |
| Finalità del trattamento |

|  |
| --- |
| Contratto di assunzione |
| Libri ed altre attività editoriali |
| Istituzione ed assistenza scolastica |
| Igiene e sicurezza del lavoro |
| Adempimento di obblighi di legge connessi a rapporti commerciali |
| Adempimento di obblighi fiscali o contabili |
| Assicurazione incidenti sul lavoro |
| Attività artistiche e culturali |
| Attività di previdenza |
| Attività turistiche e ricreative  |
| Attività sportive |
| Comunicazione multimediale |
| Indagini di mercato |
| Gestione contabile o di tesoreria  |
| Gestione Data Protection |
| Gestione dei fornitori (contratti, ordini, arrivi, fatture)  |
| Gestione del contenzioso (contratti, ordini, arrivi, fatture)  |
| Adempimenti connessi al versamento delle quote di iscrizione a sindacati |

 |
| Tipo di dati personali |

|  |
| --- |
| Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. |
| Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae |
| Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) |
| Particolari (sensibili) |
| Personali |
| Adesione a sindacati o organizzazioni a carattere sindacale |
| Amministrazione personale |
| Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) |
| Convinzioni religiose, adesioni ad organizzazioni a carattere religioso |
| Dati di comunicazione elettronica |
| Dati finanziari |
| Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) |
| Dati personali relativi a condanne penali e reati |
| Dati relativi alla famiglia e a situazioni personali |
| Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) |
| Dati relativi all'attività economica e commerciale |
| Dati sulla salute |
| Giudiziari |
| Origini razziali o etniche |
| Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) |

 |
| Categorie di interessati |

|  |
| --- |
| Docenti |
| Familiari dell'interessato |
| Collaboratori |
| Dipendenti |
| Candidati per eventuale rapporto di lavoro |
| Clienti ed utenti |
| Consulenti e liberi professionisti, anche in forma associata |
| Enti |
| Familiari degli studenti |
| Fornitori |
| Imprenditori e piccoli imprenditori |
| Iscritti in albi ed elenchi |
| Lavoratori Autonomi |
| Personale pubblico dirigenziale e magistrati |
| Potenziali dipendenti (curricula) |
| Soci associati ed iscritti |
| Studenti minorenni |
| Appartenenti all'organizzazione |

 |
| Categorie di destinatari |

|  |
| --- |
| Associazioni ed enti locali |
| Responsabili interni |
| Datore di lavoro |
| Familiari dell'interessato |
| Soggetti che svolgono attività di archiviazione della documentazione |
| Altre amministrazioni pubbliche |
| Autorità di vigilanza e controllo |
| Consulenti e liberi professionisti anche in forma associata |
| Enti locali |
| Enti previdenziali ed assistenziali |
| Enti pubblici economici |
| Enti pubblici non economici |
| Fornitori di servizi informatici |
| Fornitori di servizi amministrativi e contabili |
| Imprese di assicurazione |
| Interessati |
| Istituzione di formazione professionale  |
| Medico competente |
| Organismi sanitari, personale medico e paramedico |
| Persone autorizzate |
| Responsabili esterni |
| Rappresentante dei lavoratori per la sicurezza |
| Servizi pubblici |
| Società che effettuano il servizio di logistica di magazzino e trasporto |
| Società di gestione per il controllo delle frodi |
| Studi legali |
| Uffici giudiziari |
| Imprese |
| Società e imprese |
| Piattaforme di elaborazione |

 |
| Informativa | Si |
| Profilazione | Non necessaria |
| Dati particolari | Si |
| Consenso minori | Si |
| Frequenza trattamento | Giornaliera |
| Termine cancellazione dati | I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto in essere e per i successivi dieci anni dalla data di acquisizione degli stessi. I dati obbligatori ai fini istituzionali sono conservati ai sensi della normativa vigente verificabile presso il seguente link: http://www.archivi.beniculturali.it/index.php/cosa-facciamo/progetti-di-tutela/progetti-conclusi/item/556-archivi-delle-scuole. |
| Trasferimento dati (paesi terzi) | No |
|  Autorizzazione del Garante | Non presente |

|  |
| --- |
| Modalità di elaborazione dati: Mista - elettronica e cartacea |
| Strumenti |

|  |
| --- |
| Software gestionale |
| Equivalenti Office |
| Pacchetto Office |
| Servizi cloud |
| Servizi Google |
| Google Drive |

 |
| Strutture informatiche di archiviazione |
| Server  | Struttura interna |
| Sede di riferimento | Sede Centrale |
| Personale con diritti di accesso |

|  |
| --- |
| Fiorillo Teresa Assunta, c.f. FRLTSS67D41G190C |
| Colantoni Anna Teresa, c.f. CLNNTR61H45L117D |
| Daminato Carla, c.f. DMNCRL58M48L117V |
| Comella Roberto, c.f. CMLRRT63C03L117U |
| Salvati Angela, c.f. SLVNGL64C47L117Q |

 |
| Software utilizzati |

|  |
| --- |
| - Nuvola |
| - Spaggiari |

 |
| Strutture informatiche di backup |
| Server  | Struttura interna |
| Sede di riferimento | Sede Centrale |
| Frequenza di backup | 30 giorni |
| Tempo di storicizzazione | 365 giorni |
| Personale con diritti di accesso |

|  |
| --- |
| Fiorillo Teresa Assunta, c.f. FRLTSS67D41G190C |
| Colantoni Anna Teresa, c.f. CLNNTR61H45L117D |
| Daminato Carla, c.f. DMNCRL58M48L117V |
| Comella Roberto, c.f. CMLRRT63C03L117U |
| Salvati Angela, c.f. SLVNGL64C47L117Q |

 |
| Note |  |
| Software utilizzati |

|  |
| --- |
| - Nuvola |
| - Spaggiari |

 |

|  |
| --- |
| VALUTAZIONE DEL LIVELLO DI RISCHIO |
| PROBABILITÀ | CONSEGUENZE | LIVELLO DI RISCHIO |
| Probabile | Gravi | Rilevante |

|  |
| --- |
| MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE |
|  - Adozione di cifratura e anonimizzazione dei dati su stato di salute  - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - Dispositivi antincendio - E' applicata una gestione della password degli utenti - E' eseguita la DPIA - E' presenta una politica per la sicurezza e la protezione dei dati - Esistono procedure per l'individuazione del custode delle password - I documenti vengono firmati digitalmente - Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi - Le credenziali sono disattivate in caso di perdita della qualità - Le password sono costituite da almeno otto caratteri alfanumerici - Le password sono modificate ogni 3 mesi - Le procedure sono riesaminate con cadenza predefinita - L'impianto elettrico è certificato ed a norma - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Sistemi di allarme e di sorveglianza anti-intrusione - Sono applicate regole per la gestione delle password. - Sono definiti i ruoli e le responsabilità - Sono definiti i termini di conservazione e le condizioni di impiego dei dati. - Sono gestiti i back up - Sono stabiliti programmi di formazione e sensibilizzazione - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Viene eseguita una regolare formazione del personale |

### VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

|  |  |  |
| --- | --- | --- |
| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
| Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale | * 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.)
 | Parzialmente adeguate |
| Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati | * Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Dispositivi antincendio | * Agenti fisici (incendio, allagamento, attacchi esterni)
 | Adeguate |
| E' applicata una gestione della password degli utenti | * Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)
* Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| E' eseguita la DPIA | * Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | * Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)
* Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Esistono procedure per l'individuazione del custode delle password | * Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Parzialmente adeguate |
| I documenti vengono firmati digitalmente | * Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Impianto elettrico dotato di misure salvavita atte anche ad 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 |
| Le credenziali sono disattivate in caso di perdita della qualità | * Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)
* Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Parzialmente adeguate |
| Le password sono costituite da almeno otto caratteri alfanumerici | * Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Le password sono modificate ogni 3 mesi | * Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Le procedure sono riesaminate con cadenza predefinita | * Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | 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 elettroniche e cartacee | * Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Sistemi di allarme e di sorveglianza anti-intrusione | * Agenti fisici (incendio, allagamento, attacchi esterni)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
* Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)
 | Adeguate |
| Sono applicate regole per la gestione delle password. | * Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Sono definiti i ruoli e le responsabilità | * Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Sono definiti i termini di conservazione e le condizioni di impiego dei dati. | * 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 |
| 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)
 | Parzialmente adeguate |
| Sono stabiliti programmi di formazione e sensibilizzazione | * Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Sono utilizzati software antivirus e anti intrusione | * Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
* Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |
| Viene eseguita opportuna manutenzione | * Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)
 | Adeguate |
| Viene eseguita una regolare formazione del personale | * Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
 | Adeguate |

### VALUTAZIONE DEI RISCHI

|  |
| --- |
| PERICOLO |
| Agenti fisici (incendio, allagamento, attacchi esterni) |
| RISCHI |
| * Perdita
* Distruzione non autorizzata
 |
| VALUTAZIONE RISCHIO INTRINSECO |
| Probabilità | Conseguenza | Rischio intrinseco - Ri |
| Poco probabile | Gravi | 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 |

|  |
| --- |
| PERICOLO |
| Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) |
| RISCHI |
| * Perdita
* Distruzione non autorizzata
 |
| VALUTAZIONE RISCHIO INTRINSECO |
| Probabilità | Conseguenza | Rischio intrinseco - Ri |
| 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 | 0,25 | 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 |
| 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 |

|  |
| --- |
| 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 |
| 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 |

|  |
| --- |
| 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 | Gravi | 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 |

|  |
| --- |
| 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 | Gravi | 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