# CITTÀ METROPOLITANA DI MESSINA

## Decreto Sindacale

n. 21 del 28 FEB. 2019

**OGGETTO: Presa d'atto della "Valutazione d'impatto sulla protezione dei dati" (DPIA) e delle "Istruzioni operative di data Breach" ai sensi del GDPR 2016/679 e normativa nazionale in vigore.**

### IL SINDACO METROPOLITANO

l'anno duemiladiciannove il giorno VENTOTTO del mese di FEBBRAIO, alle ore 12,10, nella sede di Palazzo dei Leoni, con l'assistenza del Segretario Generale Avv. M. A. CAPONETTI:

**Vista** l'allegata proposta di decreto relativo all'oggetto;
**Vista** la L.R. n. 15 del 04.08.2015 e successive modifiche ed integrazioni;
**Viste** le LL.RR. n. 48/91 e n. 30/2000 che disciplinano l'O.R.EE.LL.;
**Visto** il D.Lgs. n. 267/2000 e ss.mm.ii.;
**Visto** il D.P. della Regione Siciliana n. 576/GAB del 02/07/2018, che all'art. 2 recita: *"le funzioni del Sindaco Metropolitano e della Conferenza Metropolitana sono esercitate dal Sindaco pro-tempore del Comune di Messina On.le Cateno De Luca";*
**Visti** i pareri favorevoli, espressi ai sensi dell'art. 12 della L.R. n. 30 del 23.12.2000:

- per la regolarità tecnica, dal Dirigente proponente;
- per la regolarità contabile e per la copertura finanziaria della spesa, dal Dirigente della II Direzione – Servizi Finanziari;

### DECRETA

**APPROVARE** la proposta di decreto indicata in premessa, allegata al presente atto per farne parte integrante e sostanziale, facendola propria integralmente.
**DARE ATTO** che il presente provvedimento è immediatamente esecutivo a norma di legge.

# CITTÀ METROPOLITANA DI MESSINA

## Proposta di Decreto Sindacale

## della VII DIREZIONE "Affari Territoriali e Comunitari"

### Servizio "Servizi Informatici"

**OGGETTO: Presa d'atto della "Valutazione d'impatto sulla protezione dei dati" e delle "Istruzioni operative di Data Breach" ai sensi del GDPR 2016/679 e normativa nazionale in vigore.**

**PREMESSO** che in data 4 Maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea n. L 119/2016 il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, indicato anche come *"General Data Protection Regulation"* (GDPR);

**CHE** lo stesso è stato dichiarato immediatamente esecutivo e direttamente applicabile negli ordinamenti degli Stati membri;

**CHE** la Città Metropolitana di Messina con il Decreto Sindacale n.161 del 16/07/2018, mediante procedura sul MEPA, ha designato quale Responsabile della Protezione dei Dati (DPO) la società "IT & T" rappresentata dall'ing. Giuseppe Bono;

**EVIDENZIATO** che i dati personali conservati, trattati, inviati o comunque gestiti dalle Pubbliche Amministrazioni possono essere soggetti a perdita, distruzione, manomissione, diffusione indebita anche in conseguenza di attacchi informatici, accessi abusivi, incidenti o eventi rovinosi come incendi o altre calamità, con grave pregiudizio per la privacy degli interessati cui si riferiscono i dati;

**RILEVATO** che tra i documenti compilati dal Responsabile della Protezione dei Dati spiccano per la loro rilevanza la "Valutazione di impatto sulla protezione dei dati", relativa alla gravità delle conseguenze cui andrebbe incontro un trattamento dei dati nel caso in cui si verificasse una violazione nelle sue misure di protezione, nonchè il manuale delle "Istruzioni operative di Data Breach" in cui vengono dettagliate le procedure da adottare per la gestione della violazione dei dati;

**PRESO ATTO** che tali documenti sono stati visionati e personalizzati in funzione delle

esigenze dell'Ente da parte dei "Servizi Informatici" della VII Direzione;

**ATTESO** che con proprio atto, prot. n.1730/SG del 14/12/2018, il Segretario Generale avv. Maria Angela Caponetti ha già emanato le *"Istruzioni operative per gli incaricati del trattamento in materia di applicazione del GDPR (Regolamento UE 679/16)".*

**Si propone che il Sindaco Metropolitano**

**DECRETI**

**Prendere atto** dei documenti "Valutazione d'impatto sulla protezione dei dati" e "Istruzioni operative di Data Breach" qui allegati, che costituiscono parte integrante del presente atto.

Il Funzionario
*dott. Giacomo Lucà*

Il Dirigente
*ing. Armando Cappadonia*

**SI ALLEGANO I SEGUENTI DOCUMENTI:**

1. Valutazione d'impatto sulla protezione dei dati
2. Istruzioni operative di Data Breach

Oggetto: **Presa d'atto della "Valutazione d'impatto sulla protezione dei dati" e delle "Istruzioni operative di Data Breach" ai sensi del GDPR 2016/679 e normativa nazionale in vigore.**

**PARERE DI REGOLARITÀ TECNICA**

Ai sensi e per gli effetti dell'art. 12 della L.R. 23-12-2000 n. 30 e ss.mm.ii., si esprime parere:

FAVOREVOLE

In ordine alla regolarità tecnica della superiore proposta di decreto.

Addì 31/1/19

IL DIRIGENTE
Il Dirigente
ing. A. Cappadonia

Si dichiara che la proposta non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria dell'Ente e pertanto non è dovuto il parere di regolarità contabile.

Addì 31/1/19

IL DIRIGENTE
Il Dirigente
ing. A. Cappadonia

**PARERE DI REGOLARITÀ CONTABILE**

Ai sensi e per gli effetti dell'art. 12 della L.R. 23-12-2000 n. 30 e ss.mm.ii., si esprime parere:

In ordine alla regolarità contabile della superiore proposta di decreto.

Addì_____

IL RAGIONIERE GENERALE

Ai sensi del D.Lgs 267/2000, si attesta la copertura finanziaria della superiore spesa.

Addì_____

IL RAGIONIERE GENERALE

**Decreto Sindacale n.** 21 **del** 28 FEB. 2019

Oggetto: PRESA D'ATTO DELLA "VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI" (DPIA) E DELLE "ISTRUZIONI OPERATIVE DI DATA BREACH" AI SENSI del GDPR 2016/679 e NORMATIVA NAZIONALE IN VIGORE.

**Letto, confermato e sottoscritto.**

**Il Sindaco Metropolitano**

.....
(Dott. On. Cateno DE LUCA)

**Il Segretario Generale**

.....
AVV. M. A. CAPONETTI

---

**CERTIFICATO DI PUBBLICAZIONE**

Il sottoscritto Segretario Generale,

CERTIFICA

Che il presente decreto _____ pubblicato all'Albo on-line dell'Ente il _____ e per quindici giorni consecutivi e che contro lo stesso _____ sono stati prodotti, all'Ufficio preposto, reclami, opposizioni o richieste di controllo.

Messina, _____

IL SEGRETARIO GENERALE

_____

---

E' copia conforme all'originale da servire per uso amministrativo.

Messina, _____

IL SEGRETARIO GENERALE

_____

# VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

*ai sensi del GDPR 2016/679 e normativa nazionale in vigore*

| | |
|---|---|
| Azienda/Organizzazione | **Città Metropolitana di Messina** |

| | |
|---|---|
| **TITOLARE** | Sindaco Pro-Tempore della Città di Messina |

| | |
|---|---|
| **SEDE** | Sede Principale<br>Corso Cavour 86, 98122<br>Messina - ME |

Data revisione: 08/01/2019

# 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:

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 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:

$$LR = P \times C$$

**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 | 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

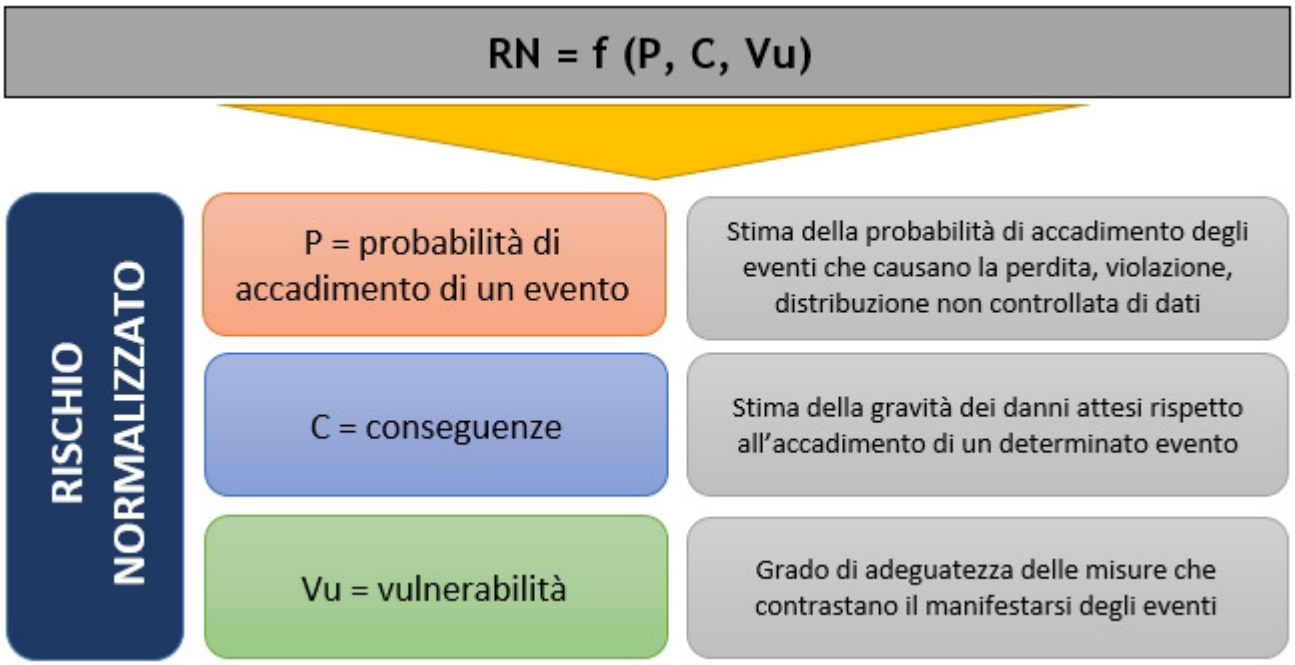
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione 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<br>• Distruzione non autorizzata |
| Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | • Perdita<br>• Distruzione non autorizzata |
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |
| Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |
| Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |
| Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• 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.

## 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

- Sindaco Città Metropolitana
- Segreteria Generale
- 1^ Direzione Affari Generali - Legali e del Personale
- 2^ Direzione Affari Finanziari e Tributari
- 3^ Direzione Viabilità Metropolitana
- 4^ Direzione Servizi Tecnici Generali
- 5^ Direzione Sviluppo Economico e Politiche Sociali
- 6^ Direzione Ambiente
- 7^ Direzione Affari Territoriali e Comunitari
- Polizia Metropolitana

## Sindaco Città Metropolitana

| Personale coinvolto | |
|---|---|
| **Titolare del trattamento** | DE LUCA CATENO |
| **Persone autorizzate** | CARACCIOLO ROBERTO |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| Processo di trattamento | |
|---|---|
| **Descrizione** | Sindaco della Città Metropolitana di Messina |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Adesione a partiti od organizzazioni a carattere politico<br>Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc.<br>Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali)<br>Giudiziari<br>Opinioni politiche<br>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 |
| **Categorie di interessati** | Cittadini |
| **Categorie di destinatari** | Altre amministrazioni pubbliche<br>Enti locali |
| **Informativa** | Si |
| **Profilazione** | Si |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| Modalità di elaborazione dati: Mista - elettronica e cartacea | |
|---|---|
| **Strumenti** | Software gestionale |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |
| **Strutture informatiche di backup** | |

| Server Interno | Struttura interna |
|---|---|
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| VALUTAZIONE DEL LIVELLO DI RISCHIO | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

| MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE |
|---|
| - E' eseguita la DPIA |

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| E' eseguita la DPIA | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| PERICOLO | | |
|---|---|---|
| Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |

| | | |
|---|---|---|
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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**

## Segreteria Generale

| Personale coinvolto | |
|---|---|
| **Responsabile del trattamento** | CAPONETTI MARIA ANGELA |
| **Persone autorizzate** | ABRAMO PATRIZIA<br><br>D'ANGELO GIOVANNA<br><br>GARGOTTA GIOVANNI<br><br>ALESSI GIANCARLO<br><br>DE SALVO SABASTIANO MASSIMO<br><br>CARACCIOLO ROBERTO<br><br>FRENI ROSA |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| Processo di trattamento | |
|---|---|
| **Descrizione** | Servizio Contratti<br>Servizio Ispettivo<br>Servizio Controllo della Performance<br>Servizio Trasparenza e URP |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Amministrazione personale<br>Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc.<br>Dati finanziari<br>Dati relativi all'attività economica e commerciale<br>Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali)<br>Giudiziari<br>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<br>Personali<br>Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro)Codice fiscale ed altri numeri di identificazione personale (carte sanitarie)Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)Particolari (sensibili)PersonaliCurriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc.GiudiziariLavoro |

| | |
|---|---|
| | (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 |
| **Categorie di interessati** | Cittadini<br>Dipendenti |
| **Categorie di destinatari** | Enti locali<br>Enti previdenziali ed assistenziali<br>Altre amministrazioni pubbliche |
| **Informativa** | Si |
| **Profilazione** | Si |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |
| **Strutture informatiche di backup** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

| **MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE** |
|---|
| - E' eseguita la DPIA |

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| E' eseguita la DPIA | Compromissione informazioni | Parzialmente |

| | | |
|---|---|---|
| | (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | adeguate |

## VALUTAZIONE DEI RISCHI

| PERICOLO | | |
|---|---|---|
| Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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**

## 1^ Direzione Affari Generali - Legali e del Personale

| Personale coinvolto | |
|---|---|
| **Responsabile del trattamento** | TRIPODO ANNA MARIA |
| **Persone autorizzate** | TURRISI MARIA GIOVANNA<br>CHILLEMI RITA<br>MICELI SANTA<br>MOLLURA ANTONINO<br>DE LUCA ENZA<br>TUCCIO GIUSEPPA<br>ARIGO' GIUSEPPINA<br>BAGALA' GAETANO<br>CALABRO' MARIANO<br>IELASI CAMILLA<br>SALVATORE ANGELA<br>SIDOTI CARMELINA<br>DE LEO ANGELO<br>LUCIANI ANTONIO<br>PIRERA ANTONINO<br>MEO PATRIZIA<br>AJELLO SALVATORE<br>CALAPAI LETTERIA<br>DELIRO GIUSEPPE<br>DI CARLO MARIA PIA<br>FILOCAMO FORTUNATA<br>IEMMO MATILDE<br>PARISI ELEONORA<br>PELLIZZIERI CORINNE<br>TRIPODO ROCCO<br>MILETI PIETRO PAOLO<br>PUGLISI ROSA |

| | |
|---|---|
| | ARENA GIANDOMENICO<br>CARAMELI CARMELA<br>DI BARTOLO NICOLA<br>DI GENNARO NUNZIATINA<br>GUERRERI GIOVANNI<br>LA CORTE ROSSELLA<br>PAVIA RITA<br>SICILIANO DOMENICA<br>BRANCA ROBERTO<br>DE SALVO GIUSEPPE<br>ZONA ROSARIO<br>TRIMARCHI MARGHERITA<br>INFONDENTI STEFANO<br>CARACCIOLO ROBERTO |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Svolge atti di supporto alla Direzione in merito ad atti di valenza generale e programmatori. Garantisce la comunicazione tra la Direzione e i relativi Servizi ed Uffici per lo scambio di informazioni e comunicazioni, privilegiando lo strumento telematico ed informatico. Si occupa della gestione della corrispondenza e del registro delle determinazioni e delle disposizioni. |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Personali |
| **Categorie di interessati** | |
| **Categorie di destinatari** | Enti locali<br>Altre amministrazioni pubbliche |
| **Informativa** | Si |
| **Profilazione** | Si |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |
| **Trasferimento dati (paesi terzi)** | No |

| | |
|---|---|
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |
| **Strutture informatiche di backup** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- E' applicata una procedura per la gestione degli accessi
- 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
- Le credenziali sono disattivate se inutilizzate per sei mesi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate ogni 3 mesi
- Sono definiti i ruoli e le responsabilità
- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Vengono registrati e conservati i Log file
- Viene effettuata la registrazione ed il controllo degli accessi
- Viene eseguita una regolare formazione del personale

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| 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.) | Parzialmente adeguate |

| | | |
|---|---|---|
| Dispositivi antincendio | Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |
| E' applicata una procedura per la gestione degli accessi | Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' eseguita la DPIA | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente 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 |
| Le credenziali sono disattivate se inutilizzate per sei mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso | Parzialmente adeguate |

| | | |
|---|---|---|
| | non autorizzato di strumentazione, ecc.) | |
| Le password sono costituite da almeno otto caratteri alfanumerici | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Le password sono modificate ogni 3 mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono definiti i ruoli e le responsabilità | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono gestiti i back up | Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Agenti fisici (incendio, allagamento, attacchi esterni)<br>Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Parzialmente adeguate |
| Sono utilizzati software antivirus e anti intrusione | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Vengono registrati e | Compromissione informazioni | Parzialmente |

| | | |
|---|---|---|
| conservati i Log file | (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | adeguate |
| Viene effettuata la registrazione ed il controllo degli accessi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Viene eseguita una regolare formazione del personale | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| **PERICOLO** | | |
|---|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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** |
| 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 |
|---|
| 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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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**

## 2^ Direzioni Affari Finanziari e Tributari

| Personale coinvolto | |
|---|---|
| **Responsabile del trattamento** | RANIERI MASSIMO |
| **Persone autorizzate** | LEARDI STEFANIA<br>CAMA CATERINA<br>MILLER DAVIDE<br>FRANCICA GIUSEPPA<br>CICCIO' SALVATORE<br>NULLI MARIA GRAZIA<br>COSTA PASQUALE<br>PARISI SALVATORE<br>RUSSO FABIO<br>TODARO ROSARIA<br>GALLETTA DOMENICA<br>MAGGIO GIUSEPPE<br>CACCIOLA ANNUNZIATA<br>CUTRONEO GASPARE<br>ZAGARELLA LETTERIO<br>SURRENTI ANTONIO<br>SAMMARTINO ANTONIO<br>LO PRESTI CONCETTA<br>GRASSO GIUSEPPINA<br>BERENATO SALVATORE<br>FALLITI GIACOMINA<br>CATTAFI ROSA<br>RIPOLI TIZIANA<br>INFERRERA CONCETTA<br>BINOLLINI IGNAZIA<br>SIMONE FRANCESCO<br>RIZZO FRANCESCA |

| | |
|---|---|
| | MAGAZZU' GRAZIA |
| | SCIARRONE GIOVANNI |
| | POLLICINO ANGELA |
| | SPARACINO MARIA ROSA |
| | CANDIDO LETTERIA |
| | PARISI MARIA GRAZIA |
| | SPAMPINATO ANTONINO |
| | MANGRAVITI DOMENICA |
| | PRESTIGIOVANNI FRANCESCO |
| | GEMELLI GIUSEPPE |
| | MICALI MARIO |
| | MIANO GIUSEPPA |
| | SIMONE BRUNELLA |
| | LA MALFA MARIA LUISA |
| | SCANDURRA TEODORA |
| | MAZZULLO CINZIA |
| | MAIMONE PIETRO |
| | BELLINVIA ANTONINO |
| | RICCIARDI SALVATORE |
| | BONSIGNORE ANNA |
| | MANCUSO NATALA |
| | SALVATI CONCETTA |
| | ORIOLES ROSA |
| | SOFIA FRANCESCA |
| | CUTRONEO TERESA |
| | BONANNELLA RITA |
| | LANZAFAME FERNANDO |
| | DI STEFANO CARMELO |
| | ALIZZI ANTONINO |
| | GENTILE ANTONINA |

| | |
|---|---|
| | MICALI SALVATORE<br><br>COSTANTINO GIUSEPPE<br><br>RUGGERI TIZIANA<br><br>SCIUTTERI FLAVIA<br><br>CERTO FRANCESCO<br><br>BARDETTA NICOLA<br><br>CREMENTE GIOVANNI<br><br>CARACCIOLO ROBERTO |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Servizio Controllo di Gestione Finanziaria<br>Servizio Programmazione Finanziaria<br>Servizio Entrate<br>Servizio Patrimonio Mobiliare<br>Servizio Contabilità LL.PP. e Mutui<br>Servizio Gestione Economica del Personale |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Personali |
| **Categorie di interessati** | Cittadini |
| **Categorie di destinatari** | Altre amministrazioni pubbliche<br>Enti locali |
| **Informativa** | Si |
| **Profilazione** | Si |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Pacchetto Office |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |

| Strutture informatiche di backup | |
|---|---|
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| VALUTAZIONE DEL LIVELLO DI RISCHIO | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

| MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE |
|---|
| - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati<br>- Dispositivi antincendio<br>- E' applicata una procedura per la gestione degli accessi<br>- E' eseguita la DPIA<br>- E' presenta una politica per la sicurezza e la protezione dei dati<br>- Esistono procedure per l'individuazione del custode delle password<br>- Le credenziali sono disattivate se inutilizzate per sei mesi<br>- Le password sono costituite da almeno otto caratteri alfanumerici<br>- Le password sono modificate ogni 3 mesi<br>- Sono definiti i ruoli e le responsabilità<br>- Sono gestiti i back up<br>- Sono utilizzati software antivirus e anti intrusione<br>- Vengono registrati e conservati i Log file<br>- Viene effettuata la registrazione ed il controllo degli accessi<br>- Viene eseguita una regolare formazione del personale |

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| 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.) | Parzialmente adeguate |
| Dispositivi antincendio | Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |
| E' applicata una procedura per la gestione degli accessi | Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>Interruzione servizi (sbalzi di tensione, guasti impianto di | Parzialmente adeguate |

| | | |
|---|---|---|
| | climatizzazione, interruzione collegamenti di rete, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| E' eseguita la DPIA | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente 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 |
| Le credenziali sono disattivate se inutilizzate per sei mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>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.)<br>Azioni non autorizzate (Errori | Parzialmente adeguate |

| | | |
|---|---|---|
| | volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| Le password sono modificate ogni 3 mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono definiti i ruoli e le responsabilità | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono gestiti i back up | Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Agenti fisici (incendio, allagamento, attacchi esterni)<br>Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Parzialmente adeguate |
| Sono utilizzati software antivirus e anti intrusione | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Vengono registrati e conservati i Log file | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

| | | |
|---|---|---|
| Viene effettuata la registrazione ed il controllo degli accessi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Viene eseguita una regolare formazione del personale | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| **PERICOLO** | | |
|---|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 | | |
|---|---|---|
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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**

## 3^ Direzione Viabilità Metropolitana

| Personale coinvolto | |
|---|---|
| **Responsabile del trattamento** | ROCCAFORTE FRANCESCO |
| **Persone autorizzate** | ARENA CONO<br>CHIAIA PASQUALE<br>CRISTAUDO FRANCESCO<br>STORNANTI DOMENICO<br>SEDIA CARMELA<br>TOMASELLO SANTINO<br>CARACCIOLO ROBERTO |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| Processo di trattamento | |
|---|---|
| **Descrizione** | Servizio Protezione Civile<br>1° Servizio Viabilità Distretto Peloro/Eolie<br>2° Servizio Viabilità Distretto Costa Jonica<br>3° Servizio Viabilità Distretto Nebrodi Orientali<br>4° Servizio Viabilità Distretto Valle dell'Alcantara<br>5° Servizio Viabilità Distretto Nebrodi Occidentali<br>Servizio Speciale Espropri |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)<br>Altro<br>Personali |
| **Categorie di interessati** | Cittadini |
| **Categorie di destinatari** | Altre amministrazioni pubbliche<br>Interessati |
| **Informativa** | Si |
| **Profilazione** | Si |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

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

| | |
|---|---|
| **Strumenti** | Pacchetto Office |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |
| **Strutture informatiche di backup** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| VALUTAZIONE DEL LIVELLO DI RISCHIO | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

| MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE |
|---|
| - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati<br>- Dispositivi antincendio<br>- E' applicata una procedura per la gestione degli accessi<br>- E' eseguita la DPIA<br>- E' presenta una politica per la sicurezza e la protezione dei dati<br>- Esistono procedure per l'individuazione del custode delle password<br>- Le credenziali sono disattivate se inutilizzate per sei mesi<br>- Le password sono costituite da almeno otto caratteri alfanumerici<br>- Le password sono modificate ogni 3 mesi<br>- Sono definiti i ruoli e le responsabilità<br>- Sono gestiti i back up<br>- Sono utilizzati software antivirus e anti intrusione<br>- Vengono registrati e conservati i Log file<br>- Viene effettuata la registrazione ed il controllo degli accessi<br>- Viene eseguita una regolare formazione del personale |

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| 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.) | Parzialmente adeguate |
| Dispositivi antincendio | Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |

| | | |
|---|---|---|
| E' applicata una procedura per la gestione degli accessi | Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' eseguita la DPIA | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente 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 |
| Le credenziali sono disattivate se inutilizzate per sei mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>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.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Le password sono modificate ogni 3 mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono definiti i ruoli e le responsabilità | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono gestiti i back up | Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Agenti fisici (incendio, allagamento, attacchi esterni)<br>Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Parzialmente adeguate |
| Sono utilizzati software antivirus e anti intrusione | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Vengono registrati e conservati i Log file | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in | Parzialmente adeguate |

| | | |
|---|---|---|
| | messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| Viene effettuata la registrazione ed il controllo degli accessi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Viene eseguita una regolare formazione del personale | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| **PERICOLO** | | |
|---|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 |
|---|
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) |
| **RISCHI** |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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**

## 4^ Direzione Servizi Tecnici Generali

| Personale coinvolto | |
|---|---|
| **Responsabile del trattamento** | ROCCAFORTE FRANCESCO |
| **Persone autorizzate** | BALLARO' ANGELO<br>BOTTARO MARIA<br>SIRACUSANO MARIELLA<br>SODO GRASSO MARIA LUISA<br>LANZAFAME SERGIO<br>SPECIALE GIUSEPPE<br>SIDOTI DONATELLA<br>MINUTOLI FRANCESCO<br>PISPISA GIOVANNI<br>ROMEO NICOLA<br>ANNA NICOLO'<br>CALARCO DOMENICO<br>CHIESINI FORTUNATO<br>CORDARO ANTONINO<br>GAROFALO CARMELO<br>MARINO CATERINA<br>MARTINO GIOVANNI<br>MILIOTI STEFANO<br>PICCOLOMINI CONCETTA<br>RAFFA GIUSEPPA<br>TRIPODO ROSARIA<br>PALELLA GIUSEPPE<br>ROMANO RICCARDO<br>GIACOBBE DOMENICA M.<br>VENUTO MATTEO<br>ANTONAZZO GAETANO<br>DE LUCA ANTONINO |

| | |
|---|---|
| | MARCIANO' NICOLETTA<br>BRANCATO ANTONINO<br>COSTANZO ERMANNO<br>GIORGIANNI STEFANO<br>RUSSO GIACOMO<br>GUGLIANDOLO MARIA<br>MICELI ANTONINO<br>MANGIAPANE SANDRO<br>AlLITO PIETRO<br>CARACCIOLO ROBERTO |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Servizio Edilizia Metropolitana<br>Servizio Edilizia Scolastica<br>Servizio Prevenzione e Coordinamento Attività Datore di Lavoro<br>Servizio Autoparco |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Personali<br>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** | Cittadini |
| **Categorie di destinatari** | Altre amministrazioni pubbliche |
| **Informativa** | Si |
| **Profilazione** | Si |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |

| | |
|---|---|
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |
| **Strutture informatiche di backup** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| VALUTAZIONE DEL LIVELLO DI RISCHIO | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

| MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE |
|---|
| - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati<br>- Dispositivi antincendio<br>- E' applicata una procedura per la gestione degli accessi<br>- E' eseguita la DPIA<br>- E' presenta una politica per la sicurezza e la protezione dei dati<br>- Esistono procedure per l'individuazione del custode delle password<br>- Le credenziali sono disattivate se inutilizzate per sei mesi<br>- Le password sono costituite da almeno otto caratteri alfanumerici<br>- Le password sono modificate ogni 3 mesi<br>- Sono definiti i ruoli e le responsabilità<br>- Sono gestiti i back up<br>- Sono utilizzati software antivirus e anti intrusione<br>- Vengono registrati e conservati i Log file<br>- Viene effettuata la registrazione ed il controllo degli accessi<br>- Viene eseguita una regolare formazione del personale |

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| 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.) | Parzialmente adeguate |
| Dispositivi antincendio | Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |
| E' applicata una procedura per la gestione degli accessi | Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Parzialmente adeguate |

| | | |
|---|---|---|
| | Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| E' eseguita la DPIA | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente 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 |
| Le credenziali sono disattivate se inutilizzate per sei mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>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, | Parzialmente adeguate |

| | | |
|---|---|---|
| | ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| Le password sono modificate ogni 3 mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono definiti i ruoli e le responsabilità | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono gestiti i back up | Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Agenti fisici (incendio, allagamento, attacchi esterni)<br>Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Parzialmente adeguate |
| Sono utilizzati software antivirus e anti intrusione | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Vengono registrati e conservati i Log file | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, | Parzialmente adeguate |

| | | |
|---|---|---|
| | ecc.) | |
| Viene effettuata la registrazione ed il controllo degli accessi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Viene eseguita una regolare formazione del personale | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| **PERICOLO** | | |
|---|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 | | |
|---|---|---|
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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**

## 5^ Direzione Sviluppo Economico e Politiche Sociali

| Personale coinvolto | |
|---|---|
| **Responsabile del trattamento** | Tripodo Anna Maria |
| **Persone autorizzate** | MASTRONARDO SALVATORE<br>LA TORRE MARIA<br>CICERO BENEDETTO<br>PARISI LUIGI<br>CUTICONE MARIA PIA<br>SACCA' CATERINA<br>PREVITI GIUSEPPE<br>MALATINO ANTONINO<br>AZZOLINA PIPPO<br>CARROCCIO MARIA<br>RESTIFO LUCIANA<br>ROMEO OLIVIA<br>ANDALORO PASQUALINO<br>NICITA AGATINO<br>D'ANDREA ANTONINO<br>CORICA MARIANNA<br>GRISO ATTILIO<br>MELITA ROSALBA<br>CECCIO RITA<br>CARACCIOLO ROBERTO |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| Processo di trattamento | |
|---|---|
| **Descrizione** | Servizio Politiche del Lavoro Giovanili e Occupazionali<br>Servizio Politiche Sociali<br>Servizio Attività Produttive<br>Servizio Turismo<br>Servizio Cultura |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento** | Consenso |

| | |
|---|---|
| **per dati comuni (art. 6 GDPR)** | |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Personali |
| **Categorie di interessati** | Cittadini |
| **Categorie di destinatari** | Enti locali<br>Altre amministrazioni pubbliche |
| **Informativa** | Si |
| **Profilazione** | Si |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |
| **Strutture informatiche di backup** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- E' applicata una procedura per la gestione degli accessi
- 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
- Le credenziali sono disattivate se inutilizzate per sei mesi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate ogni 3 mesi
- Sono definiti i ruoli e le responsabilità
- Sono gestiti i back up

- Sono utilizzati software antivirus e anti intrusione
- Vengono registrati e conservati i Log file
- Viene effettuata la registrazione ed il controllo degli accessi
- Viene eseguita una regolare formazione del personale

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| 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.) | Parzialmente adeguate |
| Dispositivi antincendio | Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |
| E' applicata una procedura per la gestione degli accessi | Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' eseguita la DPIA | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori | Parzialmente adeguate |

| | | |
|---|---|---|
| | volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| 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 |
| Le credenziali sono disattivate se inutilizzate per sei mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>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.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Le password sono modificate ogni 3 mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono definiti i ruoli e le responsabilità | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono gestiti i back up | Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |

| | | |
|---|---|---|
| | Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | |
| Sono utilizzati software antivirus e anti intrusione | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Vengono registrati e conservati i Log file | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Viene effettuata la registrazione ed il controllo degli accessi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Viene eseguita una regolare formazione del personale | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| **PERICOLO** |
|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) |
| **RISCHI** |
| • Perdita<br>• Distruzione non autorizzata |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 |
|---|
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) |
| **RISCHI** |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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**

## 6^ Direzione Ambiente

| Personale coinvolto | |
|---|---|
| **Responsabile del trattamento** | CAPPADONIA ARMANDO |
| **Persone autorizzate** | VERI GRAZIA<br>DI GIORGIO GIUSEPPE<br>ADORNO GIUSEPPE<br>CUCE' CAFEO DANIELA<br>CONDORELLI ANNA<br>BOCCAFURRI UGO<br>BATTAGLIA CARMELO<br>CAPPELLO CONCETTA<br>IPSALE SALVATORE<br>MOLINO MARIA LETIZIA<br>SARLO CONCETTA<br>CARACCIOLO ROBERTO |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| Processo di trattamento | |
|---|---|
| **Descrizione** | Servizio Parchi e Riserve<br>Servizio Tutela delle Acque e dell'Aria<br>Servizio Controllo Gestione dei Rifiuti<br>Servizio qualità aria, impianti termici ed educazione ambientale<br>Servizio Ingegneria Territoriale |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Personali |
| **Categorie di interessati** | Cittadini |
| **Categorie di destinatari** | Altre amministrazioni pubbliche<br>Enti locali |
| **Informativa** | Si |
| **Profilazione** | Si |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |

| | |
|---|---|
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Pacchetto Office |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |
| **Strutture informatiche di backup** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

| **MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE** |
|---|
| - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati<br>- Dispositivi antincendio<br>- E' applicata una procedura per la gestione degli accessi<br>- E' eseguita la DPIA<br>- E' presenta una politica per la sicurezza e la protezione dei dati<br>- Esistono procedure per l'individuazione del custode delle password<br>- Le credenziali sono disattivate se inutilizzate per sei mesi<br>- Le password sono costituite da almeno otto caratteri alfanumerici<br>- Le password sono modificate ogni 3 mesi<br>- Sono definiti i ruoli e le responsabilità<br>- Sono gestiti i back up<br>- Sono utilizzati software antivirus e anti intrusione<br>- Vengono registrati e conservati i Log file<br>- Viene effettuata la registrazione ed il controllo degli accessi<br>- Viene eseguita una regolare formazione del personale |

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| 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.) | Parzialmente adeguate |

| | | |
|---|---|---|
| Dispositivi antincendio | Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |
| E' applicata una procedura per la gestione degli accessi | Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' eseguita la DPIA | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente 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 |
| Le credenziali sono disattivate se inutilizzate per sei mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori | Parzialmente adeguate |

| | | |
|---|---|---|
| | volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| Le password sono costituite da almeno otto caratteri alfanumerici | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Le password sono modificate ogni 3 mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono definiti i ruoli e le responsabilità | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono gestiti i back up | Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Agenti fisici (incendio, allagamento, attacchi esterni)<br>Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Parzialmente adeguate |
| Sono utilizzati software antivirus e anti intrusione | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

| | | |
|---|---|---|
| Vengono registrati e conservati i Log file | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Viene effettuata la registrazione ed il controllo degli accessi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Viene eseguita una regolare formazione del personale | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| **PERICOLO** | | |
|---|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 |
|---|
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) |
| **RISCHI** |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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**

## 7^ Direzione Affari Territoriali e Comunitari

| Personale coinvolto | |
|---|---|
| **Responsabile del trattamento** | CAPPADONIA ARMANDO |
| **Persone autorizzate** | LIBRO NICOLA<br><br>DONATI FERDINANDO<br><br>FURNARI CATERINA<br><br>MAIORANA ALESSANDRA<br><br>CARACCIOLO ROBERTO |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| Processo di trattamento | |
|---|---|
| **Descrizione** | Servizio Geologico<br>Servizio Pianificazione Strategica<br>Servizio Progettazione Comunitaria<br>Servizio S.I.T.R.<br>Servizi Informatici |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Personali |
| **Categorie di interessati** | Cittadini |
| **Categorie di destinatari** | Enti locali<br>Altre amministrazioni pubbliche |
| **Informativa** | Si |
| **Profilazione** | Si |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| Modalità di elaborazione dati: Mista - elettronica e cartacea | |
|---|---|
| **Strumenti** | Software gestionale |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |

| Strutture informatiche di backup | |
|---|---|
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| VALUTAZIONE DEL LIVELLO DI RISCHIO | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

| MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE |
|---|
| - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati<br>- Dispositivi antincendio<br>- E' applicata una procedura per la gestione degli accessi<br>- E' eseguita la DPIA<br>- E' presenta una politica per la sicurezza e la protezione dei dati<br>- Esistono procedure per l'individuazione del custode delle password<br>- Le credenziali sono disattivate se inutilizzate per sei mesi<br>- Le password sono costituite da almeno otto caratteri alfanumerici<br>- Le password sono modificate ogni 3 mesi<br>- Sono definiti i ruoli e le responsabilità<br>- Sono gestiti i back up<br>- Sono utilizzati software antivirus e anti intrusione<br>- Vengono registrati e conservati i Log file<br>- Viene effettuata la registrazione ed il controllo degli accessi<br>- Viene eseguita una regolare formazione del personale |

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| 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.) | Parzialmente adeguate |
| Dispositivi antincendio | Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |
| E' applicata una procedura per la gestione degli accessi | Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>Interruzione servizi (sbalzi di tensione, guasti impianto di | Parzialmente adeguate |

| | | |
|---|---|---|
| | climatizzazione, interruzione collegamenti di rete, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| E' eseguita la DPIA | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente 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 |
| Le credenziali sono disattivate se inutilizzate per sei mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>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.)<br>Azioni non autorizzate (Errori | Parzialmente adeguate |

| | | |
|---|---|---|
| | volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| Le password sono modificate ogni 3 mesi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono definiti i ruoli e le responsabilità | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono gestiti i back up | Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>Agenti fisici (incendio, allagamento, attacchi esterni)<br>Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Parzialmente adeguate |
| Sono utilizzati software antivirus e anti intrusione | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Vengono registrati e conservati i Log file | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

| | | |
|---|---|---|
| Viene effettuata la registrazione ed il controllo degli accessi | Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Viene eseguita una regolare formazione del personale | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| **PERICOLO** | | |
|---|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 | | |
|---|---|---|
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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<br>• Distruzione non autorizzata<br>• Modifica non autorizzata |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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**

## Polizia Metropolitana

| Personale coinvolto | |
|---|---|
| **Responsabile del Trattamento** | TRIOLO ANTONINO |
| **Persone autorizzate** | ANSALDO PATTI ADELE<br>ARDIZZONE BARTOLOMEO<br>ARITO LUIGI<br>BITTO GIUSEPPE<br>BRUNO DOMENICO<br>CASUBOLO CATERINA<br>CELI FRANCESCO<br>COLOMBO GIOVANNI<br>CURRO' ANTONINO<br>D'ARRIGO CONCETTA<br>DE PASQUALE MARIA<br>PALMAROSA FAZIO<br>FOTIA PIETRO<br>GULLETTA FRANCESCO<br>LOMBARDO ROBERTO<br>MARCHELLO GIUSEPPE<br>PERDICHIZZI SANTINA<br>RUGGERI GIOVANNI<br>SOTTILE GIOVANNA<br>CARACCIOLO ROBERTO |
| **Partners - Responsabili esterni** | |
| **Altro** | |
| | |

| Processo di trattamento | |
|---|---|
| **Descrizione** | Il Corpo di Polizia Metropolitana esercita l'insieme delle attività di polizia demandate dalla legge alle competenze della Provincia, che non siano espressamente riservate all'Autorità Statale o ad altre Autorità.<br><br>Esso ha competenza su tutto il territorio della provincia di Messina: un'area di circa 3.200 km² sulla quale, al 2009, era stimata una popolazione residente di circa 650.000 abitanti. |

| | |
|---|---|
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | |
| **Tipo di dati personali** | Personali |
| **Categorie di interessati** | Cittadini |
| **Categorie di destinatari** | Enti locali<br>Altre amministrazioni pubbliche |
| **Informativa** | Non necessaria |
| **Profilazione** | Non necessario |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Semestrale |
| **Termine cancellazione dati** | I dati saranno tenuti per il tempo necessario alle mansioni dell'ente e verranno archiviate a norma di legge per 10 anni |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale |
| **Strutture informatiche di archiviazione** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Software utilizzati | - Cartella Condivisa |
| **Strutture informatiche di backup** | |
| **Server Interno** | Struttura interna |
| Sede di riferimento | Sede Principale |
| Frequenza di backup | 1 giorni |
| Tempo di storicizzazione | 30 giorni |
| Personale con diritti di accesso | CARACCIOLO ROBERTO |
| Note | |
| Software utilizzati | - Cartella Condivisa |

| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- E' applicata una procedura per la gestione degli accessi
- 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
- Le credenziali sono disattivate se inutilizzate per sei mesi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate ogni 3 mesi
- Sono definiti i ruoli e le responsabilità

- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Vengono registrati e conservati i Log file
- Viene effettuata la registrazione ed il controllo degli accessi
- Viene eseguita una regolare formazione del personale

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| 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.) | Parzialmente adeguate |
| Dispositivi antincendio | • Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |
| E' applicata una procedura per la gestione degli accessi | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' eseguita la DPIA | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori | Parzialmente adeguate |

| | | |
|---|---|---|
| | volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| 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 |
| Le credenziali sono disattivate se inutilizzate per sei mesi | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• 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.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Le password sono modificate ogni 3 mesi | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono definiti i ruoli e le responsabilità | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono gestiti i back up | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Inadeguate |

| | | |
|---|---|---|
| | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | |
| Sono utilizzati software antivirus e anti intrusione | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Vengono registrati e conservati i Log file | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Inadeguate |
| Viene effettuata la registrazione ed il controllo degli accessi | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Inadeguate |
| Viene eseguita una regolare formazione del personale | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| **PERICOLO** |
|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) |
| **RISCHI** |
| • Perdita<br>• Distruzione non autorizzata |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 | 1 | Rilevante |

| PERICOLO |
|---|
| Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) |
| **RISCHI** |
| • Perdita<br>• Distruzione non autorizzata |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 |
|---|
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) |
| **RISCHI** |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 | 1 | Rilevante |

| PERICOLO |
|---|

| Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | | |
|---|---|---|
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 | 1 | Rilevante |

| **PERICOLO** | | |
|---|---|---|
| Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 | 1 | Rilevante |

| **PERICOLO** | | |
|---|---|---|
| Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |

| Probabilità | Conseguenza | Rischio intrinseco - Ri |
|---|---|---|
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*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 | 1 | Rilevante |

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

# Città Metropolitana di Messina

**(*ai sensi della L.R. n. 15 del 4 agosto 2015*)**

**Disposizioni in materia di applicazione del GDPR (Regolamento UE 679/16)**
**istruzioni operative Data Breach**

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche. Qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è di 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre l'eventuale comunicazione agli interessati deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato. Il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), l'imposizione di sanzioni amministrative secondo l'art. 83 GDPR e della normativa nazionale in vigore.

Per **"Violazione di dati personali (data breach)"**, ai sensi dell'Art. 4 p.12 del GDPR, si intende *"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"*.

La violazione di dati è un particolare tipo di incidente di sicurezza per effetto del quale il titolare non è in grado di garantire il rispetto dei principi previsti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza; quindi comprendere se l'incidente ha impatto sulle informazioni e, infine, se tra le informazioni compromesse dall'incidente vi siano dati personali.

Al riguardo l'art. 33 p.2 del GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare senza ingiustificato ritardo il titolare. E al p.5 viene sancito il dovere per il titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art.34 del GDPR, invece, prescrive, in casi di violazione di dati personali suscettibili di rischi elevatri per i diritti e le libertà della persone fisiche, l'obbligo di comunicazione all'interessato da parte del titolare senza ingiustificato ritardo.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.
Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza: quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità: quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità: quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente**: la notifica al Garante non è obbligatoria.
- **Rischio presente**: è necessaria la notifica al Garante.
- **Rischio elevato**: In presenza di rischi "elevati", è necessario darne comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, ad esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, inerenti le abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare il previsto "modello segnalazione data breach", disponibile sul sito "Garante per la Protezione dei dati Personali".