COMUNE DI CAPANNORI

# Documento di Valutazione di impatto sulla protezione dei dati

# (DPIA - *DATA PROTECTION IMPACT ASSESSMENT*)

Redatto ai sensi dell'articolo 35 del Regolamento UE 679/2016 e delle Linee Guida WP248 rev. 01 adottate il 4 Aprile 2017 in materia di valutazione d'impatto sulla protezione dei dati e determinazione delle possibilità che il trattamento "possa presentare un rischio elevato".

**REDAZIONE del documento**

**Titolare del trattamento:**

***Comune di Capannori***

Legale rappresentante: dott. Luca Menesini (in qualità di Sindaco)

Responsabile della protezione dei dati (RPD/DPO): dott. Giuseppe Ascione

**SEDE**

*Piazza Aldo Moro, n. 1 – Capannori (LU)*

**DATA**

***28 dicembre 2018***

**MOTIVAZIONE DELLA VALUTAZIONE**

Il presente documento viene elaborato sulla scorta dell'articolo 35 del Regolamento UE 679/2016. La valutazione d'impatto si rende necessaria alla luce di un'attenta autoanalisi compiuta circa il trattamento dei dati personali.

Il **Comune di Capannori**, con sede in Piazza Aldo Moro, n. 1 (LU), quale Ente Pubblico, in ragione del trattamento su larga scala di categorie particolari di dati personali di cui all'art. 9, paragrafo 1, e di dati relativi a condanne penali e a reati di cui all'art. 10 del Regolamento UE 679/2016, del trattamento dei dati tramite l'utilizzo di nuove tecnologie, *ex* art. 35 co. 1 del medesimo Regolamento, ed in particolare tramite l'utilizzo di sistemi di videosorveglianza e di pubblicazione on-line di tali dati, nonché, ai sensi e per gli effetti dell'art. 35 comma 4 del Reg. UE 679/2016, in ragione del trattamento su larga scala di dati avente carattere estremamente personale, del trattamento non occasionale di dati relativi a soggetti vulnerabili, del trattamento che comporta lo scambio tra diversi titolari di dati su larga scala con modalità telematiche, ritiene necessario procedere ad una valutazione di impatto, stante il rischio elevato che tali trattamenti possano avere sui diritti e le libertà delle persone fisiche.

**DEFINIZIONI**

**Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 del Regolamento UE 2016/679).

**Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4 del Regolamento (UE) 2016/679).

**Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4 del Regolamento (UE) 2016/679).

**Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4 del Regolamento (UE) 2016/679).

**Destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento (art. 4 del Regolamento (UE) 2016/679).

**Terzo**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al

trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art. 4 del Regolamento (UE) 2016/679).

**Rischio**: scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità (Linee-guida 17/EN WP248).

**Gestione del rischio**: l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio (Linee-guida 17/EN WP248).

"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario"[1].

La valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

- "*una descrizione dei trattamenti previsti e delle finalità del trattamento";*
- *"una valutazione della necessità e proporzionalità dei trattamenti";*
- *"una valutazione dei rischi per i diritti e le libertà degli interessati";*
- *"le misure previste per:*
    - "*affrontare i rischi*"*;*
    - "*dimostrare la conformità al presente regolamento".*

In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

- stabilendo il contesto: *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";*
- *valutando i rischi: " valutare la particolare probabilità e gravità del rischio";*

[1] Cfr. anche il Considerando 84:*"[l]'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento".*

- *trattando i rischi: "attenuando tale rischio", "assicurando la protezione dei dati personali" e "dimostrando la conformità al presente regolamento".*

Nota: la valutazione d'impatto sulla protezione dei dati svolta ai sensi del Regolamento generale sulla protezione dei dati è uno strumento per gestire i rischi per i diritti degli interessati, di conseguenza, adotta la loro prospettiva, come avviene in taluni settori (ad esempio, la sicurezza sociale). Al contrario, la gestione del rischio in altri settori (ad esempio in quello della sicurezza delle informazioni) è incentrata sull'organizzazione.

**CRITERI PER LA VALUTAZIONE DI RISCHIO E DI IMPATTO**

In esplicazione di quanto detto nel presente documento, sono riportati gli elementi previsti dalla normativa vigente (art. 35, comma 7):

1. La descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
2. La valutazione della necessità e proporzionalità dei trattamenti;
3. La valutazione dei rischi per i diritti e le libertà degli interessati;
4. Le misure previste per affrontare i rischi.

Le principali norme di riferimento in materia definiscono il rischio come “effetto dell’incertezza” (UNI EN ISO 9000) ovvero “effetto dell’incertezza sugli obiettivi” (UNI ISO 31000), dove l’effetto è uno scostamento da quanto atteso.

Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento e della verosimiglianza del suo verificarsi, dove per verosimiglianza (o possibilità) si intende la plausibilità di un accadimento ipotizzabile e, per conseguenze, si intendono gli esiti di un evento che influenza gli obiettivi.

La verosimiglianza può essere descritta come probabilità (o frequenza, con riferimento ad un dato intervallo di tempo). Le conseguenze di un evento possono avere effetti positivi o negativi sugli obiettivi.

Pertanto, la definizione di rischio contenuta nelle Linee-guida 17/EN WP 248 è sovrapponibile con queste definizioni: “scenario descrittivo di un evento e delle relative conseguenze, che sono stimate

in termini di gravità e probabilità".

Pertanto il rischio può essere espresso come funzione di G (*gravità delle conseguenze) e di* P (*probabilità di accadimento dell'evento), cioè:*

**R= f (G, P)**

ove:

R = *entità del rischio*

G = *gravità delle conseguenze*

P = *probabilità di accadimento dell'evento*

Si assume in particolare che la funzione per determinare il rischio sia espressa dal prodotto di probabilità e gravità/rilevanza delle conseguenze, ovvero:

**R (rischio) = P (probabilità) x G (gravità/rilevanza)**

La procedura di valutazione dei rischi può essere riassunta come definito di seguito.

Ogni possibile minaccia viene analizzata sotto i seguenti profili:

- ✓ valutazione intrinseca della **probabilità** di accadimento dell'evento, in una scala da 1 a 4;
- ✓ valutazione della **gravità** delle conseguenze, in una scala da 1 a 4.

Per ogni possibile rischio identificato, come indicato al paragrafo 2.4 della "Procedura per la valutazione di impatto sulla protezione dei dati", è effettuata la valutazione dell'entità del rischio.

La valutazione è corretta (ossia ricalcolata) in presenza di misure di prevenzione e opportunità identificate e adeguatamente attuate, in relazione ai diversi aspetti esaminati. Si valuta così il rischio residuo, ossia il rischio che residua a seguito del trattamento del rischio stesso.

Per valutare la gravità, si tengono in considerazione il danno per la reputazione, la discriminazione, il furto d'identità, le perdite finanziarie, i danni fisici o psicologici, la perdita di controllo dei dati, altri svantaggi economici o sociali e, infine, l'impossibilità di esercitare diritti, servizi o opportunità.

**Criteri di attribuzione dei livelli di Probabilità e Gravità.**

| | | | | |
|---|---|---|---|---|
| **R (entità del rischio)** | **Probabilità** | Alta | **4** | Esiste una correlazione diretta tra la situazione rilevata ed il verificarsi dell'evento.<br><br>Si sono già verificati eventi per la stessa situazione rilevata nel medesimo luogo, in ambienti simili o in situazioni simili.<br><br>Il verificarsi dell'evento non susciterebbe alcuno stupore nell'organizzazione. |
| | | Media | **3** | La situazione rilevata può provocare l'evento anche se non in modo automatico o diretto.<br><br>E' noto qualche episodio in cui si è verificato l'evento.<br><br>Il verificarsi dell'evento susciterebbe una moderata sorpresa nell'organizzazione. |
| | | Bassa | **2** | La situazione rilevata può provocare l'evento al contemporaneo verificarsi di particolari condizioni.<br><br>Sono noti rari episodi già verificatisi.<br><br>Il verificarsi dell'evento susciterebbe una discreta sorpresa nell'organizzazione. |
| | | Estremamente bassa/non rilevante | **1** | La situazione rilevata può provocare l'evento per concomitanza di più eventi poco probabili indipendenti.<br><br>Non sono noti episodi già verificatisi. |

| | | | | |
|---|---|---|---|---|
| | | | | Il verificarsi dell'evento susciterebbe incredulità. |
| | **Gravità** | Alta | 4 | Seria violazione della privacy di un interessato.<br><br>Alto impatto su altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione), con compromissione della fruizione. Conseguenze significative irreversibili o non eliminabili (minaccia per la vita, perdita o sospensione del rapporto di lavoro, danno finanziario ingente). |
| | | Media | 3 | Violazione della privacy di un interessato con significativo disagio.<br><br>Impatto su altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione, incolumità della vita) che, in concomitanza con altri elementi, potrebbe comprometterne la fruizione. Conseguenze ripristinabili con un certo dispendio di risorse. |
| | | Bassa | 2 | Violazione della privacy di un interessato con basso impatto (es. la violazione comporta un disturbo/disagio facilmente ripristinabile).<br><br>Nessuna violazione di altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di |

| | | | | |
|---|---|---|---|---|
| | | | | coscienza e di religione). |
| | | Estremamente bassa/non rilevante | 1 | Impatto irrilevante per la privacy di un interessato.<br><br>Nessuna violazione di altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione). |

Il titolare del trattamento ed i soggetti di cui sopra, a seguito della valutazione condotta, effettuano la ponderazione dei rischi.

La ponderazione del rischio è definita come il processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio, per determinare se il rischio e/o la sua espressione quantitativa sia accettabile o tollerabile. La ponderazione del rischio agevola la decisione circa il trattamento del rischio, ossia il processo per modificare il rischio. La decisione sugli interventi necessita di stabilire a priori quale sia il livello di **rischio accettabile Ra**, in modo che si individuino le situazioni di intervento prioritarie, che presentano cioè un livello di rischio superiore al valore ritenuto accettabile (R>Ra).

La quantificazione del **rischio accettabile R < Ra** avviene in base alla tabella sottostante.

**Area del rischio accettabile**

**R = P X G**

**Probabilità (P)**

| | | | | | |
|---|---|---|---|---|---|
| Alta | 4 | 4 (eccezione) | 8 | 12 | 16 |
| Media | 3 | 3 | 6 | 9 | 12 |
| Bassa | 2 | 2 | 4 | 6 | 8 |
| Estrem. bassa / non rilevante | 1 | 1 | 2 | 3 | 4 |
| | | 1 | 2 | 3 | 4 |
| **Gravità (G)** | | Estrem. bassa / non rilevante | Bassa | Media | Alta |

La matrice in tabella individua graficamente quelli che si considerano rischi non accettabili, ovvero quelli per cui è richiesto un intervento di miglioramento tale da riportare la situazione al di sotto della soglia di accettabilità. In base alla matrice dei rischi si individuano come **non accettabili** tutti quei **rischi che risultano avere valori di P x G superiori a 4**, unica eccezione le situazioni che si riferiscono ad un alto livello di probabilità (P = 4). Poiché non si considera accettabile alcun tipo di danno, neppure di lieve entità, qualora si ritenga il suo verificarsi estremamente probabile.

La tabella che segue riporta i giudizi attribuiti alle classi di rischio. In base a quanto sopra detto, risultano **non accettabili**[2] i rischi classificati come **medio o alto**, oltre a tutti i rischi con un alto livello di probabilità (P = 4).

| | | |
|---|---|---|
| **R (entità del rischio) normalizzata** | **I ≥ 6** | **RISCHIO ALTO** |
| | **4 ≤ I ≤ 5** | **RISCHIO MEDIO** |
| | **2 ≤ I ≤ 3** | **RISCHIO BASSO** |
| | **I ≤ 1** | **RISCHIO ESTREMAMENTE BASSO, NON RILEVANTE** |

[2] Il Regolamento (UE) 2016/679 considera non accettabile il rischio "elevato", che nella presente classificazione su quattro livelli accorpa anche il livello di rischio medio.

Le carenze eventualmente evidenziate sono oggetto di **misure tecniche e organizzative e/o programmi di miglioramento** definiti al fine di **ridurre il rischio ad un livello accettabile**, secondo il criterio di accettabilità enunciato.

Tali misure e programmi tengono conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento.

**INDIVIDUAZIONE DEL TRATTAMENTO**

Ai sensi dell'art. 30 del Regolamento UE 2016/679, il titolare del trattamento, insieme al RPD/DPO agli eventuali responsabili del trattamento e ad altre funzioni coinvolte provvedono a determinare le tipologie di trattamenti di dati personali effettuati dall'organizzazione o per conto di essa, mantenendo aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità.

Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento, e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di

cui all'articolo 32, paragrafo 1, del Regolamento.

Tali informazioni sono documentate nel "Registro delle attività del trattamento", conservato in formato elettronico nello spazio su server denominato "Registro dei trattamenti". L'accesso al Registro è consentito al Titolare, ai Responsabili, al RPD e ai soggetti abilitiati, individuati dai responsabili. Le informazioni contenute nel Registro sono aggiornate in caso di modifiche significative e/o riesaminate, se necessario.

Per questa sezione relativa alla descrizione dei trattamenti previsti e delle finalità del trattamento si rinvia al documento "Registro del Trattamento".

Sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea); in particolare la struttura per il trattamento dei dati utilizza sia strumenti informatici che cartacei.

- L'utilizzazione cartacea e la dotazione di strumenti fisici di conservazione dei dati si rendono necessarie per la corretta gestione degli adempimenti e per l'attività dell'Ente con l'adozione delle seguenti misure di sicurezza:

- limitazione al solo personale autorizzato dell'attività di trattamento dei dati;

- limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo;

- limitazione dell'attività di trattamento dei dati (in particolare di quelli sensibili o particolari ex artt. 9 e 10 Reg. n. 679/2016) all'interno dei locali protetti dell'Ente;

- attività di revisione delle nomine di Responsabili e autorizzati;

- formazione e sensibilizzazione sul tema di tutto il personale dipendente

- Procedura per l'esercizio dei diritti;

- Procedura di *data breach*;

- dotazione di sistemi di allarme (con eventuale collegamento con le forze dell'ordine o con i servizi di vigilanza);

- dotazione di sistemi di videosorveglianza;

– uscierato;

– chiusura delle porte di accesso degli edifici;

– chiusura delle porte di accesso dei locali/uffici;

– serrature agli arredi;

Il ricorso a un'infrastruttura informatica si rende necessaria per la corretta gestione degli adempimenti e per l'attività della struttura con l'adozione delle misure di sicurezza di seguito indicate:

- sistemi di autenticazione mediante credenziali;

- password;

- aggiornamento periodico dei programmi;

- antivirus;

-firewall;

- salvataggio dei dati;

- allestimento di architetture per il backup automatico dotate di funzionalità di "disaster recovery";

- sistema di Intrusion Detection (IDS);

- dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server;

- salvataggi periodici dei dati su supporti alternati;

- verifica periodica della "solidità" del sistema di sicurezza adottato;

- potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza;

- protezione delle macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità;

- installazione di switch in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete;

- utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale;

- controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

- I sistemi *hardware* e *software* sono indicati nell'allegato al presente documento (allegato 1).

## VALUTAZIONE SULLA NECESSITÀ E LA PROPORZIONALITÀ DEL TRATTAMENTO

• Sono state determinate le misure previste per garantire il rispetto del Regolamento, ai sensi e per gli effetti dell'articolo 35, paragrafo 7, lettera d) e del considerando 90):

1. Informative ai soggetti interessati;
2. Richiesta del consenso quando necessario e previsto dalla legge;
3. Nomine interne di Autorizzato, Responsabile, Responsabile del trattamento esterno, Responsabile per la Protezione dei dati;
4. Regole scritte per il trattamento dei dati;
5. Registro di *accountability* (o di rendicontazione);
6. Procedura di *data breach*;
7. Adozione di misure di sicurezza tecniche, organizzative e logistiche adeguate;
8. Procedure per la *'privacy by design'* e *'privacy by default'*;
9. Formazione.

• Sono state determinate le misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di un attento monitoraggio delle tipologie di trattamento e delle modalità di utilizzo e precisamente:

1. Adempimenti di legge;
2. Adempimenti contrattuali;

3. Adempimenti o necessità precontrattuali;
4. Richiesta del consenso ove necessario;
5. Adeguata cautela nella comunicazione e pubblicazione dei dati personali;
6. Divieto di diffusione dei dati personali;
7. Trattamento per finalità di difesa giudiziale.

• Sono state individuate finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b)) attraverso la stesura di informative ben dettagliate, differenziate, diffuse sul sito istituzionale dell'Ente, con la richiesta del consenso, se necessario e non sostituibile da criteri alternativi;

• È stato rispettato il principio di liceità del trattamento (articolo 6), attraverso la valutazione delle finalità e di criteri alternativi al consenso. Preponderante è l'uso dei dati per motivi contrattuali, precontrattuali, per adempimenti di legge e per motivi di interesse pubblico o connessi all'esercizio di pubblici poteri;

• I dati personali sono adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c)): i dati personali vengono selezionati al momento della raccolta sulla base della minimizzazione e cioè richiedendo e registrando solo dati necessari ed indispensabili ai fini degli adempimenti di legge o delle finalità contrattuali;

• È stata prevista una limitazione della conservazione (articolo 5, paragrafo 1, lettera e)), con individuazione del tempo di conservazione sulla base degli obblighi di legge;
• Sono state adottate misure che contribuiscono ai diritti degli interessati: adozione di una procedura dettagliata e pubblicata sul sito, alla sezione privacy, come da allegato 2;
• Sono state fornite informazioni all'interessato (articoli 12, 13 e 14): rese per il tramite di informative rilasciate di persona, pubblicate "online" o affisse nei luoghi di raccolta dei dati o nei form di raccolta;

• Sono stati previsti i seguenti diritti:

- diritto di accesso e portabilità dei dati (articoli 15 e 20);
- diritto di rettifica e di cancellazione (articoli 16, 17 e 19);
- diritto di opposizione e di limitazione del trattamento (articoli 18 e 19);
- diritto di revoca del consenso e diritto di proporre reclamo all'Autorità di controllo.

Tutti diritti garantiti per il tramite della procedura di cui all'allegato 2 - conosciuta dai dipendenti e resa pubblica – e della creazione di una casella e-mail, dedicata a ricevere dette istanze, le quali devono essere valutate nei termini previsti dal Regolamento.

- Sono stati disciplinati i rapporti con i Responsabili del trattamento (articolo 28): redazione e consegna di atti di nomina ai Responsabili esterni con indicazione nei relativi contratti di incarico, fornitura ed appalto delle garanzie richieste, degli obblighi e delle responsabilità. Richiesta di audit periodica, su segnalazione o a campione, verso i Responsabili esterni.

- Sono state previste garanzie riguardanti trattamenti internazionali (capo V).

Per quanto attiene alla "consultazione preventiva" (articolo 36): a seguito del parere del DPO, circa la presente DPIA, si valuterà l'eventuale consultazione preventiva al Garante Privacy. In linea generale, laddove si dovessero presentare trattamenti dei dati che presentano rischi per le libertà ed i diritti dell'interessato, si valuterà preventivamente se sia necessaria la consultazione preventiva all'Autorità Garante della privacy.

**VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEI SOGGETTI INTERESSATI**

- I rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)): i rischi valutati ed indicati nella tabella di valutazione dei rischi sono stati debitamente valutati e considerati. In particolare i rischi potrebbero essere così riassunti:
  - rischio di distruzione
  - rischio di perdita
  - rischio di modifica
  - rischio di divulgazione non autorizzata
  - rischio di accesso non consentito

ai dati personali trasmessi, conservati o comunque trattati (art. 32, comma 2).

- L'origine, la natura, la particolarità e la gravità dei rischi (cfr. Considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati.

**ORIGINE INTERNA ED ESTERNA**

1) Vi sono rischi prospettabili come causati dal **comportamento degli operatori/dipendenti difforme** (per dolo o colpa). Con questi si intende la possibilità di:

1- Furto di credenziali di autentificazione che potrebbe comportare un accesso non autorizzato alle banche dati, ai pc e agli archivi contenenti il trattamento dati in formato cartaceo;

2- Carenza di consapevolezza, distrazione o incuria nell'esecuzione dell'ufficio che potrebbe determinare perdita, diffusione dei dati, il loro danneggiamento e più in generale un trattamento illecito e non corrispondente alla finalità;

3- Comportamenti sleali, dolosi che potrebbero comportare un rischio alto di diffusione del dato e conseguente trattamento non corrispondente alla finalità;

4- Errore materiale nell'esecuzione dell'ufficio che potrebbe determinare il rischio di trattamenti illeciti, diffusioni, omissioni nel corretto e lecito trattamento;

5- Errori umani nella gestione della struttura fisica, con ciò pensando a perdita e danneggiamento dei dati per mancato inserimento del sistema di allarme, nella mancata revisione del sistema di antincendio, fino alla fortuita dimenticanza di aperture che facilitano l'ingresso furtivo di terzi non autorizzati.

2) Vi sono rischi prospettabili come **causati dolosamente, ma anche derivanti da caso fortuito, da eventi esterni che coinvolgono gli strumenti di lavoro e la struttura** (sia informatici che materiali). Con questi si intende la possibilità di:

1 - Attacco da parte di virus al sistema informatico, che potrebbe causare danneggiamento ai software e conseguente danneggiamento, perdita, diffusione non autorizzata dei dati;

2 - Attacco *criptolocker* che potrebbe causare danneggiamento ai software e conseguente danneggiamento, perdita, diffusione non autorizzata dei dati.

3 - *Spamming*, anche in tale ipotesi si verificherebbe danneggiamento ai software e conseguente danneggiamento, perdita, diffusione non autorizzata dei dati;

4 - Malfunzionamento per vetustà degli elaboratori e degli strumenti di lavoro, il rischio anche in questo caso è il danneggiamento, perdita, diffusione non autorizzata dei dati;

5 - Accesso ai locali da parte di soggetti non autorizzati. L'intrusione con conseguente furto dei soli dati o della strumentazione comporterebbe perdita, diffusione non autorizzata dei dati;

6 - Accessi in rete non autorizzati. Il rischio in parola è anche ricollegabile agli interventi da remoto sulle macchine, da parte dell'assistenza tecnica, ai software, ai computer e ai server, che potrebbe condurre anche in modo del tutto inconsapevole alla cancellazione di dati, alla loro diffusione,

cancellazione.

3) Vi sono rischi prospettabili come causati da **eventi causali, prevedibili pur in astratto.**

Con tale tipologia di rischio si intende la possibilità di eventi distruttivi naturali o artificiali che possono causare la perdita e il danneggiamento delle macchine delle strutture e, conseguentemente, dei dati trattati e ivi conservati.

**NATURA DOLOSA E COLPOSA**

I rischi sopra prospettati possono essere ricondotti a possibili eventi di natura sia **dolosa** che **colposa**.

**PARTICOLARITÀ RISCHI INFORMATICI E CARTACEI**

Come evidenziato, si considerano come fonti di rischio al momento prevedibili (cfr. Considerando 90):

- errore umano dell'operatore e del personale dipendente;
- rischi provenienti dall'esterno (virus, *troianhorse*, *ramsomware*, intrusione informatica ecc.);
- interazione materiale con la struttura (e gli strumenti), cartacea e informatica, di soggetti terzi non autorizzati e con intenti dolosi (sottrazione per furto fisico di hardware, software o strumenti elettronici, documenti cartacei);
- eventi fortuiti anche di origine naturale e catastrofale.

Sono state individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati: le minacce prevalenti sono determinate da potenziali virus esterni, strumenti di intrusione fraudolenta, errore umano, furto e sottrazione si strumenti elettronici e archivi o fascicoli cartacei.

**GRAVITÀ; TIPOLOGIA DI CONSEGUENZE (perdita, accesso, danno di immagine, ecc.)**

Sono stati, come evidenziato, individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati: in tale circostanza l'impatto potenziale consiste nella conoscenza di informazioni e dati personali trattati all'interno della struttura che possono causare un potenziale (da provare) rischio per la libertà, la riservatezza dei soggetti interessati e nei casi di dati sensibili anche della dignità della persona.

- Si considerano le fonti di rischio (cfr. Considerando 90), che sono le seguenti:

- errore umano;
- rischi provenienti dall'esterno (virus, *troianhorse*, *ramsomware*, intrusione informatica ecc.);

- sottrazione per furto fisico di hardware, software o strumenti elettronici;

Sono stimate, dunque, la probabilità e la gravità per determinarne il livello di rischio (Considerando 90):

**1)Trattamento su larga scala di categorie particolari di dati di cui all'art. 9, paragrafo 1 o di dati relativi a condanne penali e a reati di cui all'art. 10 (art. 35, par. 3, lett. b) del Regolamento UE 679/2016)**

**VALUTAZIONE SUI DATI INFORMATICI**
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **2** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **3** | Rischio distruzione **6** | | | | |
| Probabilità perdita **2** | | Rischio perdita **4** | | | |
| Probabilità modifica **3** | | | Rischio modifica **6** | | |
| Probabilità divulgazione non autorizzata **3** | | | | Rischio divulgazione non autorizzata **6** | |
| Probabilità accesso non consentito **3** | | | | | Rischio accesso non consentito **6** |

**MISURE NECESSARIE**

- **Rischio distruzione:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall; dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; allestimento di architetture per il backup automatico ; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite relativamente (solo sui server Linux);

- **Rischio perdita:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale;

utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

- **Rischio perdita:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall; dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

- **Rischio divulgazione non autorizzata:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall; dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

- **Rischio accesso non consentito:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall; dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

**VALUTAZIONE SUI DATI INFORMATICI**
**(Dopo l'applicazione delle misure necessarie )**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **2** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **4** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Probabilità perdita **1** | | Rischio perdita **2** | | | |
| Probabilità modifica **1** | | | Rischio modifica **2** | | |
| Probabilità divulgazione non autorizzata **2** | | | | Rischio divulgazione non autorizzata **4** | |
| Probabilità accesso non consentito **1** | | | | | Rischio accesso non consentito **2** |

**VALUTAZIONE SUI DATI CARTACEI**
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **2** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **3** | Rischio distruzione **6** | | | | |
| Probabilità perdita **4** | | Rischio perdita **8** | | | |
| Probabilità modifica **3** | | | Rischio modifica **6** | | |
| Probabilità divulgazione non autorizzata **4** | | | | Rischio divulgazione non autorizzata **8** | |
| Probabilità accesso non consentito **4** | | | | | Rischio accesso non consentito **8** |

**MISURE NECESSARIE**

- **Rischio distruzione:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale sono custoditi i dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare trattamento dei dati *ex* artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente; procedura per l'esercizio dei diritti; Procedura di *data breach*; (dotazione di sistemi di allarme (con collegamento con il personale in reperibilità); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura delle porte di accesso degli edifici; attivazione rilevatori di fumo; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre (solo al piano terra).

- **Rischio perdita:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare dei dati di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (con collegamento al personale in reperibilità); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura delle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre (solo per il piano terra).

- **Rischio modifica:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 del Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente; procedura per l'esercizio dei diritti; Procedura di *data breach;* dotazione di sistemi di allarme; dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura delle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre (solo per il piano terra).

- **Rischio divulgazione non autorizzata:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare dei dati di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente; Procedura per l'esercizio dei diritti; Procedura di *data breach;* dotazione di sistemi di allarme; dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura delle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre.

- **Rischio accesso non consentito:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente; Procedura per l'esercizio dei diritti; Procedura di *data breach;* dotazione di sistemi di allarme; dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre.

**VALUTAZIONE SUI DATI CARTACEI**
**(Dopo l'applicazione delle misure necessarie)**

| | Gravità distruzione | Gravità perdita | Gravità modifica | Gravità divulgazione non autorizzata | Gravità accesso non consentito |
|---|---|---|---|---|---|
| | **2** | **2** | **2** | **2** | **2** |

| | | | | | |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **4** | | | | |
| Probabilità perdita **1** | | Rischio perdita **2** | | | |
| Probabilità modifica **1** | | | Rischio modifica **2** | | |
| Probabilità divulgazione non autorizzata **2** | | | | Rischio divulgazione non autorizzata **4** | |
| Probabilità accesso non consentito **1** | | | | | Rischio accesso non consentito **2** |

## 2) Sorveglianza sistematica su larga scala di una zona accessibile al pubblico *ex* art. 35, par. 3, lett. c, Regolamento UE 679/2016

**VALUTAZIONE SUI DATI INFORMATICI**
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **3** | Gravità perdita **3** | Gravità modifica **3** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **3** |
|---|---|---|---|---|---|
| Probabilità distruzione **3** | Rischio distruzione **9** | | | | |
| Probabilità perdita **3** | | Rischio perdita **9** | | | |
| Probabilità modifica **2** | | | Rischio modifica **6** | | |
| Probabilità divulgazione non autorizzata **4** | | | | Rischio divulgazione non autorizzata **12** | |
| Probabilità accesso non consentito **4** | | | | | Rischio accesso non consentito **12** |

**MISURE NECESSARIE**

- **Rischio distruzione:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall; dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

- **Rischio perdita:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall; dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

- **Rischio modifica:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall; dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

- **Rischio divulgazione non autorizzata:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall; dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

- **Rischio accesso non consentito:**controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall; dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

## VALUTAZIONE SUI DATI INFORMATICI
**(Dopo l'applicazione delle misure necessarie )**

| | Gravità distruzione **2** | Gravità perdita **3** | Gravità modifica **3** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **4** | | | | |
| Probabilità perdita **1** | | Rischio perdita **3** | | | |
| Probabilità modifica **1** | | | Rischio modifica **3** | | |
| Probabilità divulgazione non autorizzata **1** | | | | Rischio divulgazione non autorizzata **3** | |
| Probabilità accesso non consentito **1** | | | | | Rischio accesso non consentito **2** |

## VALUTAZIONE SUI DATI CARTACEI
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **3** | Rischio distruzione **6** | | | | |
| Probabilità perdita **4** | | Rischio perdita **8** | | | |
| Probabilità modifica **3** | | | Rischio modifica **6** | | |
| Probabilità divulgazione non autorizzata **4** | | | | Rischio divulgazione non autorizzata **12** | |
| Probabilità accesso non consentito **4** | | | | | Rischio accesso non consentito **8** |

## MISURE NECESSARIE

- **Rischio distruzione:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (già collegato con il personale in reperibilità); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; serrature a tutti gli arredi.
- **Rischio perdita:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10

Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (già collegato con il personale in reperibilità); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; serrature a tutti gli arredi .

- **Rischio modifica:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (già collegato con il personale in reperibilità); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; serrature a tutti gli arredi.
- **Rischio divulgazione non autorizzata:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (già collegato con il personale in reperibilità); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; serrature a tutti gli arredi.
- **Rischio accesso non consentito:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (già collegato con il personale in reperibilità); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; serrature a tutti gli arredi.

**VALUTAZIONE SUI DATI CARTACEI**
**(Dopo l'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **2** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **4** | | | | |
| Probabilità perdita **1** | | Rischio perdita **2** | | | |
| Probabilità modifica **1** | | | Rischio modifica **2** | | |
| Probabilità divulgazione non autorizzata **2** | | | | Rischio divulgazione non autorizzata **4** | |

| | | |
|---|---|---|
| Probabilità accesso non consentito **1** | | Rischio accesso non consentito **2** |

## 3) Trattamento che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 35, par. 1, Regolamento UE 679/2016: pubblicazione on-line dei dati

**VALUTAZIONE SUI DATI INFORMATICI**
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | **Rischio distruzione 4** | | | | |
| Probabilità perdita **2** | | **Rischio perdita 4** | | | |
| Probabilità modifica **2** | | | **Rischio modifica 4** | | |
| Probabilità divulgazione non autorizzata **2** | | | | **Rischio divulgazione non autorizzata 6** | |
| Probabilità accesso non consentito **1** | | | | | **Rischio accesso non consentito 2** |

**MISURE NECESSARIE**

**Rischio distruzione:** Interventi di formazione dei dipendenti sull'informatica di base, sulle applicazioni gestionali in uso, sulle normative relative al trattamento dei dati personali (Reg. UE e del d.lgs. n. 196/2003 come modificato dal d.lgs. n. 101/2018), sulle problematiche della sicurezza (Misure minime di sicurezza Agid); sensibilizzazione di tutto il personale dipendente alle problematiche connesse al trattamento dei dati e alle relative conseguenze derivanti dell'inosservanza delle norme citate; emanazione di direttive e/o regolamenti che diano istruzioni di comportamento e modalità operative da tenere, sufficientemente elastiche per adattarsi alla maggior parte delle situazioni ma invece rigide e stringenti per le situazioni giudicate ad alto rischio; emanazione di direttive e/o sensibilizzazione delle tecniche di redazione degli atti; adozione di un Regolamento interno/Codice etico/Mansionario/Disciplinare sull'utilizzo degli strumenti informatici; diffusione delle Linee guida del Garante in materia di pubblicazione on line dei dati.

**Rischio perdita:** Interventi di formazione dei dipendenti sull'informatica di base, sulle applicazioni gestionali in uso, sulle normative relative al trattamento dei dati personali (Reg. UE e del d.lgs. n. 196/2003 come modificato dal d.lgs. n. 101/2018), sulle problematiche della sicurezza (Misure minime di sicurezza Agid); sensibilizzazione di tutto il personale dipendente alle problematiche connesse al trattamento dei dati e alle relative conseguenze derivanti dell'inosservanza delle norme citate; emanazione di direttive e/o regolamenti che diano istruzioni di comportamento e modalità operative da tenere, sufficientemente elastiche per adattarsi alla maggior parte delle situazioni ma invece rigide e stringenti per le situazioni giudicate ad alto rischio; emanazione di direttive e/o sensibilizzazione delle tecniche

di redazione degli atti; adozione di un Regolamento interno/Codice etico/Mansionario/Disciplinare sull'utilizzo degli strumenti informatici; diffusione delle Linee guida del Garante in materia di pubblicazione on line dei dati.

**Rischio modifica:** Interventi di formazione dei dipendenti sull'informatica di base, sulle applicazioni gestionali in uso, sulle normative relative al trattamento dei dati personali (Reg. UE e del d.lgs. n. 196/2003 come modificato dal d.lgs. n. 101/2018), sulle problematiche della sicurezza (Misure minime di sicurezza Agid); sensibilizzazione di tutto il personale dipendente alle problematiche connesse al trattamento dei dati e alle relative conseguenze derivanti dell'inosservanza delle norme citate; emanazione di direttive e/o regolamenti che diano istruzioni di comportamento e modalità operative da tenere, sufficientemente elastiche per adattarsi alla maggior parte delle situazioni ma invece rigide e stringenti per le situazioni giudicate ad alto rischio; emanazione di direttive e/o sensibilizzazione delle tecniche di redazione degli atti; adozione di un Regolamento interno/Codice etico/Mansionario/Disciplinare sull'utilizzo degli strumenti informatici; diffusione delle Linee guida del Garante in materia di pubblicazione on line dei dati

**Rischio divulgazione non autorizzata:** Interventi di formazione dei dipendenti sull'informatica di base, sulle applicazioni gestionali in uso, sulle normative relative al trattamento dei dati personali (Reg. UE e del d.lgs. n. 196/2003 come modificato dal d.lgs. n. 101/2018), sulle problematiche della sicurezza (Misure minime di sicurezza Agid); sensibilizzazione di tutto il personale dipendente alle problematiche connesse al trattamento dei dati e alle relative conseguenze derivanti dell'inosservanza delle norme citate; emanazione di direttive e/o regolamenti che diano istruzioni di comportamento e modalità operative da tenere, sufficientemente elastiche per adattarsi alla maggior parte delle situazioni ma invece rigide e stringenti per le situazioni giudicate ad alto rischio; emanazione di direttive e/o sensibilizzazione delle tecniche di redazione degli atti; adozione di un Regolamento interno/Codice etico/Mansionario/Disciplinare sull'utilizzo degli strumenti informatici; diffusione delle Linee guida del Garante in materia di pubblicazione on line dei dati

**Rischio accesso non consentito:** Interventi di formazione dei dipendenti sull'informatica di base, sulle applicazioni gestionali in uso, sulle normative relative al trattamento dei dati personali (Reg. UE e del d.lgs. n. 196/2003 come modificato dal d.lgs. n. 101/2018), sulle problematiche della sicurezza (Misure minime di sicurezza Agid); sensibilizzazione di tutto il personale dipendente alle problematiche connesse al trattamento dei dati e alle relative conseguenze derivanti dell'inosservanza delle norme citate; emanazione di direttive e/o regolamenti che diano istruzioni di comportamento e modalità operative da tenere, sufficientemente elastiche per adattarsi alla maggior parte delle situazioni ma invece rigide e stringenti per le situazioni giudicate ad alto rischio; emanazione di direttive e/o sensibilizzazione delle tecniche di redazione degli atti; adozione di un Regolamento interno/Codice etico/Mansionario/Disciplinare sull'utilizzo degli strumenti informatici; diffusione delle Linee guida del Garante in materia di pubblicazione on line dei dati

**VALUTAZIONE SUI DATI INFORMATICI**
**(Dopo l'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **2** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **1** | Rischio distruzione **2** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Probabilità perdita **1** | | Rischio perdita **2** | | | |
| Probabilità modifica **1** | | | Rischio modifica **2** | | |
| Probabilità divulgazione non autorizzata **1** | | | | Rischio divulgazione non autorizzata **2** | |
| Probabilità accesso non consentito **1** | | | | | Rischio accesso non consentito **2** |

4) **Trattamento su larga scala di dati avente carattere estremamente personale**

**VALUTAZIONE SUI DATI INFORMATICI**
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **3** | Gravità perdita **3** | Gravità modifica **3** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **3** |
|---|---|---|---|---|---|
| Probabilità distruzione **3** | Rischio distruzione **9** | | | | |
| Probabilità perdita **3** | | Rischio perdita **9** | | | |
| Probabilità modifica **3** | | | Rischio modifica **9** | | |
| Probabilità divulgazione non autorizzata **4** | | | | Rischio divulgazione non autorizzata **12** | |
| Probabilità accesso non consentito **4** | | | | | Rischio accesso non consentito **12** |

**MISURE NECESSARIE**

- **Rischio distruzione:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

- **Rischio perdita:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro.

- **Rischio modifica:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro

- **Rischio divulgazione non autorizzata:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro

- **Rischio accesso non consentito:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e

gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro

**VALUTAZIONE SUI DATI INFORMATICI**
**(Dopo l'applicazione delle misure necessarie )**

| | Gravità distruzione **2** | Gravità perdita **3** | Gravità modifica **3** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **4** | | | | |
| Probabilità perdita **1** | | Rischio perdita **3** | | | |
| Probabilità modifica **1** | | | Rischio modifica **3** | | |
| Probabilità divulgazione non autorizzata **1** | | | | Rischio divulgazione non autorizzata **3** | |
| Probabilità accesso non consentito **1** | | | | | Rischio accesso non consentito **2** |

**VALUTAZIONE SUI DATI CARTACEI**
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **2** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **3** | Rischio distruzione **6** | | | | |
| Probabilità perdita **4** | | Rischio perdita **8** | | | |
| Probabilità modifica **3** | | | Rischio modifica **6** | | |
| Probabilità divulgazione non autorizzata **4** | | | | Rischio divulgazione non autorizzata **8** | |
| Probabilità accesso non consentito **4** | | | | | Rischio accesso non consentito **8** |

**MISURE NECESSARIE**

- **Rischio distruzione:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio

| |
|---|
| dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (con eventuale collegamento con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; attivazione rilevatori di fumo. |
| ▪ **Rischio perdita:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli sensibili o particolari ex artt. 9 e 10 Reg. n. 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Referenti e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di **s**istemi di allarme (con eventuale collegamento con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; attivazione rilevatori di fumo. |
| ▪ **Rischio modifica:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (con eventuale collegamento con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; attivazione di rilevatori di fumo. |
| ▪ **Rischio divulgazione non autorizzata:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. n. 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (con eventuale collegamento con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; attivazione di rilevatori di fumo. |
| ▪ **Rischio accesso non consentito:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (con eventuale collegamento |

con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; attivazione rilevatori di fumo.

**VALUTAZIONE SUI DATI CARTACEI**
**(Dopo l'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **2** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **4** | | | | |
| Probabilità perdita **1** | | Rischio perdita **2** | | | |
| Probabilità modifica **1** | | | Rischio modifica **2** | | |
| Probabilità divulgazione non autorizzata **2** | | | | Rischio divulgazione non autorizzata **4** | |
| Probabilità accesso non consentito **1** | | | | | Rischio accesso non consentito **2** |

## 5) Trattamento non occasionale di dati relativi a soggetti vulnerabili

**VALUTAZIONE SUI DATI INFORMATICI**
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **3** | Gravità perdita **3** | Gravità modifica **3** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **3** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **6** | | | | |
| Probabilità perdita **3** | | Rischio perdita **9** | | | |
| Probabilità modifica **3** | | | Rischio modifica **9** | | |
| Probabilità divulgazione non autorizzata **4** | | | | Rischio divulgazione non autorizzata **12** | |
| Probabilità accesso non consentito **4** | | | | | Rischio accesso non consentito **12** |

**MISURE NECESSARIE**

- **Rischio distruzione:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque

| |
|---|
| in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite |
| ▪ **Rischio perdita:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro |
| ▪ **Rischio modifica:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro |
| ▪ **Rischio divulgazione non autorizzata:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro |
| ▪ **Rischio accesso non consentito:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un |

sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro

**VALUTAZIONE SUI DATI INFORMATICI**
**(Dopo l'applicazione delle misure necessarie )**

| | Gravità distruzione **2** | Gravità perdita **3** | Gravità modifica **3** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **4** | | | | |
| Probabilità perdita **1** | | Rischio perdita **3** | | | |
| Probabilità modifica **1** | | | Rischio modifica **3** | | |
| Probabilità divulgazione non autorizzata **1** | | | | Rischio divulgazione non autorizzata **3** | |
| Probabilità accesso non consentito **1** | | | | | Rischio accesso non consentito **2** |

**VALUTAZIONE SUI DATI CARTACEI**
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **2** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **3** | Rischio distruzione **6** | | | | |
| Probabilità perdita **4** | | Rischio perdita **8** | | | |
| Probabilità modifica **3** | | | Rischio modifica **6** | | |
| Probabilità divulgazione non autorizzata **4** | | | | Rischio divulgazione non autorizzata **8** | |
| Probabilità accesso non consentito **4** | | | | | Rischio accesso non consentito **8** |

**MISURE NECESSARIE**

- **Rischio distruzione:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale

| |
|---|
| vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (con eventuale collegamento con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; attivazione rilevatori di fumo; sistemi di riconoscimento biometrico (impronta digitale/iride/facciale); badge per accesso selettivo del personale a determinate aree. |
| ▪ **Rischio perdita:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli sensibili o particolari ex artt. 9 e 10 Reg. n. 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Referenti e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di **s**istemi di allarme (con eventuale collegamento con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; sistemi di riconoscimento biometrico (impronta digitale/iride/facciale); attivazione rilevatori di fumo; badge per accesso selettivo del personale a determinate aree. |
| ▪ **Rischio modifica:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (con eventuale collegamento con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; sistemi di riconoscimento biometrico (impronta digitale/iride/facciale); attivazione di rilevatori di fumo; badge per accesso selettivo del personale a determinate aree. |
| ▪ **Rischio divulgazione non autorizzata:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. n. 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (con eventuale collegamento con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; sistemi di riconoscimento biometrico |

(impronta digitale/iride/facciale); attivazione di rilevatori di fumo; badge per accesso selettivo del personale a determinate aree.

- **Rischio accesso non consentito:** limitazione al solo personale autorizzato dell'attività di trattamento dei dati; limitazione al solo personale autorizzato della facoltà di accesso agli archivi e/o ad altro luogo nel quale vengano custoditi dati su supporto cartaceo; limitazione dell'attività di trattamento dei dati (in particolare di quelli di cui agli artt. 9 e 10 Reg. UE 679/2016) all'interno dei locali protetti dell'Ente; attività di revisione delle nomine di Responsabili e autorizzati; formazione e sensibilizzazione sul tema di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali; Procedura per l'esercizio dei diritti; Procedura di *data breach*; dotazione di sistemi di allarme (con eventuale collegamento con le forze dell'ordine, o servizi di vigilanza); dotazione di sistemi di videosorveglianza; guardiania/portierato; chiusura alle porte di accesso degli edifici; chiusura delle porte di accesso dei locali/uffici; serrature agli arredi; dotazione di inferriate alle finestre; sistemi di riconoscimento biometrico (impronta digitale/iride/facciale); attivazione rilevatori di fumo; badge per accesso selettivo del personale a determinate aree.

**VALUTAZIONE SUI DATI CARTACEI**
**(Dopo l'applicazione delle misure necessarie)**

| | Gravità distruzione **2** | Gravità perdita **2** | Gravità modifica **2** | Gravità divulgazione non autorizzata **2** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **4** | | | | |
| Probabilità perdita **1** | | Rischio perdita **2** | | | |
| Probabilità modifica **1** | | | Rischio modifica **2** | | |
| Probabilità divulgazione non autorizzata **2** | | | | Rischio divulgazione non autorizzata **4** | |
| Probabilità accesso non consentito **1** | | | | | Rischio accesso non consentito **2** |

## 6) Trattamento che comporta lo scambio tra diversi titolari di dati su larga scala con modalità telematiche

**VALUTAZIONE SUI DATI INFORMATICI**
**(Prima dell'applicazione delle misure necessarie)**

| | Gravità distruzione **3** | Gravità perdita **3** | Gravità modifica **3** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **3** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **6** | | | | |
| Probabilità perdita **3** | | Rischio perdita **9** | | | |
| Probabilità modifica **3** | | | Rischio modifica **9** | | |

| | | | |
|---|---|---|---|
| Probabilità divulgazione non autorizzata **4** | | Rischio divulgazione non autorizzata **12** | |
| Probabilità accesso non consentito **4** | | | Rischio accesso non consentito **12** |

**MISURE NECESSARIE**

- **Rischio distruzione:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale (maggiore rispetto a quella già in atto); aggiornamento e maggiore implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus più potenti da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro; controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

  **ELIMINARE LE MISURE SE Già IN ATTO**

- **Rischio perdita:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro

- **Rischio modifica:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro

- **Rischio divulgazione non autorizzata:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro

- **Rischio accesso non consentito:** controllo degli accessi alle risorse di rete attraverso l'uso di identificativo utente e password da aggiornarsi periodicamente con cadenza almeno semestrale; aggiornamento e implementazione periodica dei programmi; antivirus; firewall; salvataggio dei dati; backup; protezione della rete dell'Ente da accessi esterni non autorizzati, con implementazione di firewall e di un sistema di Intrusion Detection (IDS); dotazione di antivirus da installarsi su tutti i computer dell'Ente; dotazione di gruppi di continuità per la protezione degli apparati di rete e dei server; salvataggi periodici dei dati su supporti alternati; verifica periodica della "solidità" del sistema di sicurezza adottato; allestimento di architetture per il backup automatico dotate di funzionalità di "*disaster recovery*"; potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza; proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità; installazione di *switch* in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete; utilizzo esclusivo e di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale; utilizzo di screen saver dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro

**VALUTAZIONE SUI DATI INFORMATICI**
**(Dopo l'applicazione delle misure necessarie )**

| | Gravità distruzione **2** | Gravità perdita **3** | Gravità modifica **3** | Gravità divulgazione non autorizzata **3** | Gravità accesso non consentito **2** |
|---|---|---|---|---|---|
| Probabilità distruzione **2** | Rischio distruzione **4** | | | | |
| Probabilità perdita **1** | | Rischio perdita **3** | | | |
| Probabilità modifica **1** | | | Rischio modifica **3** | | |
| Probabilità divulgazione non autorizzata **1** | | | | Rischio divulgazione non autorizzata **3** | |
| Probabilità accesso non consentito **1** | | | | | Rischio accesso non consentito **2** |

## MISURE PREVISTE PER AFFRONTARE I RISCHI

- Sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7): si vedano in proposito le misure di sicurezza informatiche di cui all'allegato 1.
- Le altre misure ritenute adeguate per contrastare i rischi individuati sono le seguenti:

- Procedure di Privacy Policy;
- Controlli interni del DPO;
- Regole scritte circa il trattamento dei dati per i soggetti autorizzati;
- Nomine scritte e responsabilizzazione dei Responsabili esterni;

- Le parti interessate sono coinvolte: sono stati coinvolti prevalentemente i ns. dipendenti e nella procedura dei diritti dell'interessato abbiamo dato la ns. disponibilità a ricevere suggerimenti circa la ns. Privacy Policy o protezione dei dati da parte dei ns. *"interessati"*.

- Si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2): questo viene sempre coinvolto nelle decisioni della struttura e viene richiesta la sua opinione professionale su singole questioni o quesiti che hanno a che fare con il trattamento dei dati personali.

Anche il presente documento verrà sottoposto al suo vaglio finale.

- Vengono raccolte le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9), attraverso la "Procedura dei diritti dell'interessato".

**CONCLUSIONI**

Si ritiene che le contromisure adottate a fronte di un rischio iniziale, determinato come alto, possano ragionevolmente abbassarlo ad un livello di sicura gestibilità da parte del Titolare.
In quest'ottica, si ritiene superflua, in accordo con il DPO, la consultazione preventiva dell'Autorità Garante, ai sensi e per gli effetti dell'art. 36 Regolamento UE 679/2016, in considerazione anche della disponibilità dell'Ente all'adozione di un graduale piano di adeguamento per assicurare la migliore sicurezza e protezione dei dati trattati da parte del Comune di Capannori.