COMUNE DI TORRI IN SABINA

PROVINCIA DI RIETI

Data revisione	16/06/2022

Regolamento in materia di protezione dati personali

Capo I - Disposizioni generali

1. Finalità

1. Il Comune di Torri in Sabina effettua i trattamenti dei dati personali nel rispetto delle disposizioni normative e regolamentari in materia di protezione delle persone fisiche, con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, attenendosi a principi di liceità, correttezza, trasparenza e riservatezza.

2. In ossequio all'art.5 del Regolamento UE 2016/679 (d'ora in avanti RGPD), i dati personali oggetto di trattamento sono:

a) trattati in modo lecito, corretto e trasparente;

b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);

d) esatti e, se necessario, aggiornati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore al conseguimento delle finalità per cui sono trattati, al termine del quale potranno essere conservati, con le modalità e nel rispetto delle disposizioni normative in materia, nel caso di ulteriori obblighi di conservazione previsti da disposizioni di legge o per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;

f) trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti, o dalla perdita, dalla distruzione o da danni accidentali.

2. Oggetto

Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Torri in Sabina.

3. Definizioni

Ai fini del presente Regolamento si intende per:

RGPD o GDPR: Regolamento Generale Protezione Dati Personali

Titolare: 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

RPD (o DPO): Responsabile Protezione Dati Personali

Responsabile esterno 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

Interessato: la persona fisica a cui si riferiscono i dati personali

Incaricato: è il soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali

Data Breach (violazione dei dati personali): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

4. Presupposti di liceità del trattamento

I trattamenti sono effettuati dal Comune di Torri in Sabina sulla base dei seguenti presupposti di liceità:

1. esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

   Rientrano in questo ambito i trattamenti compiuti per:

   g) l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;

   h) la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;

   i) l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate dalla legge al Comune di Torri in Sabina;

2. adempimento di un obbligo legale al quale è soggetto il Comune di Torri in Sabina. La finalità del trattamento è stabilita dalla stessa fonte normativa che lo disciplina;
3. esecuzione di un contratto con soggetti interessati;
4. per specifiche finalità, diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Capo II - Modello organizzativo

5. Titolare del trattamento

1. Il Comune di Torri in Sabina, rappresentato ai fini previsti dal RGPD dal Sindaco, è il Titolare del trattamento dei dati personali (di seguito, il "Titolare") raccolti anche in banche dati, digitali o cartacee.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD:
    a) liceità, correttezza e trasparenza;
    b) limitazione della finalità e minimizzazione dei dati;
    c) esattezza;
    d) limitazione della conservazione;
    e) integrità e riservatezza.
3. Il Titolare mette in atto le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati, per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del RGPD e tutte le comunicazioni e informazioni occorrenti per il loro esercizio.
4. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio mediante analisi della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
5. Il Titolare provvede a:
    a) nominare il Responsabile della protezione dei dati (RPD o DPO);
    b) individuare, nell'ambito della propria responsabilità, gli Incaricati del trattamento, quali persone ammesse a compiere operazioni sui dati personali, come definito nel Registro dei trattamenti.
    c) nominare Responsabili esterni del trattamento, di cui all'art. 28 del RGPD ovvero soggetti pubblici o privati che trattano dati personali, anche particolari, per conto del Titolare, e che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo che il trattamento soddisfi i requisiti previsti dal Regolamento UE e garantisca la tutela dei dati dell'interessato
6. Il Titolare è contitolare del trattamento, ai sensi dell'art. 26 del RGPD, nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune di Torri in Sabina da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento.
7. Il Comune di Torri in Sabina favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto

rispetto da parte del Titolare del trattamento.

6. Responsabile della protezione dati (RPD o DPO)

1. Il Responsabile della protezione dei dati (di seguito, RPD) è individuato nella figura unica di un professionista o di una società, nel rispetto delle prescrizioni recate dal Codice degli appalti in materia di contratti di servizio. In entrambi i casi il soggetto deve possedere dei requisiti specificati dagli artt. 37 e 38 del RGPD.
2. Il Responsabile della protezione dei dati è incaricato dei seguenti compiti:
    a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati;
    b) fungere da supporto alle Strutture competenti sulle richieste di accesso civico generalizzato per tutti gli aspetti relativi alla protezione dei dati personali, ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE 2016/679;
    c) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
    d) rendere una consulenza idonea, scritta od orale, anche nella individuazione dei rapporti intercorrenti con soggetti terzi in materia di protezione dei dati;
    e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione;
    f) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
    g) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;
    h) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del Responsabile della protezione dei dati.
3. La figura del Responsabile della protezione dei dati è incompatibile con chi determina le finalità o i mezzi del trattamento e con il ruolo di fornitore dell'Ente tranne nel caso in cui l'attività di fornitura sia da considerarsi quale ausilio e supporto allo svolgimento delle attività in capo al Responsabile della protezione dei dati medesimo.

In particolare, risultano con la stessa incompatibili:

a) il Responsabile per la prevenzione della corruzione e per la trasparenza;
b) qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

4. Il Responsabile della protezione dei dati dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

   Il Titolare fornisce al Responsabile della protezione dei dati le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti.

   In particolare, al Responsabile della protezione dei dati sono assicurati:

   - il supporto attivo per lo svolgimento dei compiti da degli organi di natura amministrativa e politica, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa, di bilancio e di Piano della performance;
   - le risorse finanziarie, infrastrutturali e di funzionamento (sede, attrezzature, strumentazione) nonché di personale, attraverso la collaborazione dell'Ufficio Privacy; accesso alle articolazioni funzionali dell'Ente per fornire il supporto, le informazioni e gli input essenziali.

5. Il Responsabile della protezione dei dati opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti e non deve ricevere istruzioni in merito al loro svolgimento, né sull'interpretazione da dare a una specifica questione riguardante la normativa sulla protezione dei dati personali. Ferma restando l'indipendenza nello svolgimento di detti compiti, il Responsabile della protezione dei dati riferisce direttamente al Titolare od al Responsabile del trattamento. Nel caso in cui siano rilevate dal Responsabile della protezione dei dati o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso Responsabile della protezione dei dati, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

7. Responsabile esterno del trattamento

1. I soggetti pubblici o privati che trattano dati personali, anche particolari, per conto del Titolare, e che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo che il trattamento soddisfi i requisiti previsti dal Regolamento UE e garantisca la tutela dei dati dell'interessato, assumono il ruolo di Responsabili esterni del trattamento, di cui all'art. 28 del RGPD, mediante atti giuridici in forma scritta.
2. I rapporti tra il Titolare ed i Responsabili esterni sono disciplinati dagli atti di cui al comma 1, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del Responsabile esterno del trattamento e le modalità di trattamento. Tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
3. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla normativa e ai compiti affidatigli dal Titolare del Trattamento.
4. Qualora l'Ente proceda alla nomina di Responsabili esterni dovrà prevedere, in sede di sottoscrizione del contratto di servizio, che gli uffici comunali di riferimento sottoscrivano anche il relativo atto di nomina.

8. Incaricati del trattamento

1. Titolare del Trattamento individua, nell'ambito della propria responsabilità, gli Incaricati del trattamento, quali persone ammesse a compiere operazioni sui dati personali, come definito nel Registro dei trattamenti.
2. Nell'atto di individuazione, il Titolare del Trattamento fa riferimento agli specifici ambiti di attività, o all'elenco dei trattamenti di dati personali, cui i singoli Incaricati sono preposti.
3. Tutti gli incaricati del trattamento prendono visione della seguente documentazione:
    - Disciplinare sull'utilizzo degli strumenti informatici
    - Istruzioni operative per gli incaricati del trattamento dei dati personali
    - Procedura per la gestione delle istanze degli interessati
    - Procedura data Breach

Capo III – Sicurezza e protezione dati personali

9. Sicurezza del trattamento

1. Il Titolare del trattamento e tutti i soggetti/ruoli descritti al Capo II del presente Regolamento mettono in atto, per i distinti profili di responsabilità e di azione, misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Costituiscono misure tecniche ed organizzative che possono essere adottate, tra le altre, i sistemi di autenticazione, autorizzazione, rilevazione di intrusione, sorveglianza; di protezione (antivirus; firewall; antintrusione); sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
2. La conformità del trattamento dei dati al RGPD è dimostrata attraverso l'adozione delle misure di sicurezza adeguate oppure con l'adesione a codici di condotta approvati ovvero a meccanismi di certificazione approvati.
3. Il Comune di Torri in Sabina, attraverso i ruoli individuati nel presente Regolamento, si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure anche a coloro che agiscono per suo conto ed abbia accesso a dati personali.
4. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi adottati ai sensi del D. Lgs. 196/2003 nella versione antecedente alle modifiche apportate dal D. Lgs. 101/2018.

10. Disposizioni generali

1. Le misure tecniche ed organizzative di sicurezza poste in atto per ridurre i rischi del trattamento dei dati personali assicurano la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico (Continuità Operativa).
2. In fase di sviluppo, progettazione, selezione e utilizzo di nuove applicazioni, servizi, prodotti che trattano dati personali, verrà richiesto che le software house provvedano alla cifratura e pseudonomizzazione dei dati nell'ottica del principio di privacy by design.
3. Sono in costante verifica le procedure tecnico/organizzative finalizzate a garantire la sicurezza dei trattamenti (Disaster Recovery) quindi garantire il ripristino e la disponibilità dei dati in caso di incidente fisico che comporti la perdita del Data Center.
4. Regolarmente vengono effettuate analisi per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
5. Costituiscono misure tecniche ed organizzative:
    - le misure contenute nel presente Documento;
    - la mappatura dei processi attraverso il Registro dei trattamenti.

- l'adozione di adeguate misure di sicurezza nel caso sia richiesta la valutazione d'impatto ai sensi dell'art.35 del RGPD;
- le istruzioni fornite a chi ha accesso ai dati personali e la sensibilizzazione e la formazione dei soggetti che, a diverso titolo, vengono coinvolti nel trattamento dei dati personali, in qualità di responsabili, incaricati al trattamento, amministratori di sistema;
- la definizione, formalizzazione e implementazione di processi e regole connessi alla protezione dei dati personali quali la gestione delle misure di sicurezza e dei diritti degli interessati;
- l'adeguamento della documentazione esistente alle disposizioni normative vigenti (ad esempio informative, clausole contrattuali);
- la definizione di un sistema di controllo delle vulnerabilità dei sistemi e delle applicazioni e delle correzioni necessarie;
- i sistemi di autenticazione; i sistemi di autorizzazione; i sistemi di protezione (antivirus; firewall; antintrusione; altro);
- le misure antincendio; i sistemi di rilevazione di intrusione; i sistemi di sorveglianza; i sistemi di protezione con videosorveglianza; la registrazione degli accessi; le porte, armadi e contenitori dotati di serrature e ignifughi; i sistemi di copiatura e conservazione di archivi elettronici; le altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

6. Il Comune è inoltre impegnato in un processo di valorizzazione dell'utilizzo della rete telematica, ma è consapevole che tale impegno deve essere attuato nel pieno rispetto delle previsioni normative, dei principi di necessità, pertinenza e non eccedenza dei dati personali, del diritto all'oblio e dei diritti fondamentali della persona.
7. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali potrà essere dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
8. I nominativi ed i dati di contatto del Titolare, e del Responsabile della protezione dati sono pubblicati nella sezione "privacy" del sito istituzionale del Comune e nella sezione "Amministrazione Trasparente".

11. Analisi dei rischi

1. L'efficace protezione dei dati personali è perseguita sia al momento di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi, prodotti che comportano il trattamento di dati personali (privacy by design), sia all'atto del trattamento, garantendo che siano trattati, per impostazione predefinita (privacy by default) solo i dati necessari per ogni specifica finalità di trattamento in relazione, ad esempio, alla quantità di dati personali raccolti, alla portata del trattamento, al periodo di conservazione, all'accessibilità.
2. Le misure tecniche ed organizzative progettate e realizzate assicurano un adeguato livello di sicurezza bilanciando, da un lato, lo stato dell'arte, i costi di attuazione, la natura, l'oggetto, il contesto e le finalità del trattamento e, dall'altro, i rischi che presentano i trattamenti e la natura dei dati personali da proteggere.
3. Ferma restando la facoltà dei dirigenti di settore di individuare rischi particolari connessi ad alcune tipologie di trattamento da inserire all'interno del Registro dei trattamenti, la sottostante tabella

intende offrire un quadro sintetico generale dell'analisi dei rischi presenti nell'Ente, che tiene conto dei seguenti aspetti:

- della probabilità del verificarsi dell'evento;
- dell'eventualità di distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati;
- degli eventuali pregiudizi derivati, dei danni fisici, materiali o immateriali.

Tabella

Fattori di rischio	**Tipologia evento**	**Probabilità di verificazione dell'evento: molto alta/ alta / media / bassa / molto bassa**
Sottrazione di credenziali di autenticazione	Evento riconducibileal comportamento degli operatori	Medio/Alta
Carenza di consapevolezza, disattenzione o incuria	"	Medio/Alta (probabilità media, impatto alto, es., cancellazioneerronea dati)
Comportamenti sleali o fraudolenti	"	Medio/Bassa
Errore materiale	"	Media
Banca dati residente solo su PC e su supporti removibili contenenti dati	"	Bassa
Azione di virus o di altri programmi dannosi	Evento riconducibileall'uso di strumenti elettronici	Media
Spamming o tecniche di sabotaggio	"	Media
Malfunzionamento, indisponibilità, degrado degli strumenti	"	Bassa
Accessi esterno non autorizzato ai dati	"	Medio/Bassa
Accesso interno non autorizzato ai dati	"	Medio/ Bassa
Intercettazione di informazioni in rete	"	Medio/Bassa
Accessi non autorizzati agliuffici	Evento relativo alcontesto	Media
Accessi non autorizzati a locali/reparti ad accesso ristretto	"	Bassa
Sottrazione di supporticontenenti dati	"	Bassa
Eventi distruttivi naturali	"	Bassa
Eventi distruttivi artificiali	"	Bassa
Guasti ad impianti (es., elettrico, di climatizzazione,ecc.)	"	Bassa

Eventi riconducibili ai comportamenti degli operatori.

La valutazione “media” e “medio/alta” assegnata a ciascuna delle tipologie di evento riconducibili a fatti “colposi” e la valutazione “medio/bassa” per ciò che concerne invece i fatti “dolosi”, si fonda sulla considerazione che i rischi per la riservatezza, disponibilità e integrità dei dati o delle banche di dati, ad oggi possono assai più facilmente derivare da errori o negligenza degli operatori, legata per lo più a sotto considerazione delle problematiche e della valenza da assegnare alle attività di trattamento dei dati personali, piuttosto che da comportamenti intenzionali degli operatori stessi.

Eventi riconducibili all’uso di strumenti elettronici

Per quanto concerne la presenza di banche dati residenti solo su PC e su supporti removibili contenenti dati, la valutazione è “ bassa” in quanto il loro uso è vietato o comunque altamente sconsigliato.

Per ciò che concerne l’azione di virus o di altri programmi dannosi, la valutazione è “media” perché tutti i pc sono dotati di programmi antivirus, aggiornati in automatico quotidianamente, ma questi sistemi non sono in grado di bloccare la totalità dei virus presenti in rete.

Quanto a spamming o tecniche di sabotaggio, la probabilità dell’evento è da stimare “media”, perché nonostante la presenza di un sistema centralizzato di anti-spam, esiste sempre la possibilità che alcune e-mail passino attraverso il filtro.

Relativamente a malfunzionamento, indisponibilità, degrado degli strumenti, si segnala che il piano di sostituzione dei PC è in fase avanzata e si sta definendo un piano di aggiornamento tecnologico costante per mantenere un livello di sicurezza adeguato.

Sugli accessi esterni non autorizzati, la rete è protetta da un Firewall di nuova generazione in grado di bloccare, ed eventualmente segnalare, tentativi di intrusione dall’esterno.

Riguardo all’intercettazione di informazioni in rete, si valuta “bassa” la probabilità che possa avvenire in quanto l’accesso agli apparati di rete è protetto da password conosciute solo dagli Amministratori di Sistema, ed il traffico dati risulta criptato tramite protocollo Https.

Eventi relativi al contesto

Per ciò che concerne l’evento “sottrazione di supporti contenenti dati”, oltre a valere quanto più oltre indicato riguardo all'accesso alle sedi e uffici, si segnala che il personale ha il dovere di vigilare sull’uso della strumentazione informatica in dotazione e di utilizzarla correttamente. Al riguardo sono state impartite precise istruzioni nel Disciplinare sull'uso degli strumenti di lavoro e sul trattamento dei dati personali.

Per questo motivo, la probabilità di verificazione di tale evento è stimata “bassa”. Nondimeno i dirigenti di settore sono tenuti a sollecitare periodicamente l’attenzione del personale su questo aspetto.

Si reputa bassa la probabilità di eventi distruttivi naturali, in considerazione della valutazione delle vicende pregresse.

Eventi distruttivi artificiali non si sono mai verificati e comunque anche per essi si prevede, in via preventiva, la costante vigilanza del personale preposto.

La probabilità di verificazione dell’evento è perciò stimata “bassa”.

Per gli eventi distruttivi naturali e artificiali, si ritiene fondamentale l'attività del Servizio Prevenzione e Protezione che dovrà garantire la protezione delle aree e dei locali, con specifico riferimento ai Piani di Emergenza elaborati per la Struttura Comunale.

Relativamente ai guasti agli impianti (ad esempio guasti all'impianto elettrico), non si segnalano situazione di rischio particolare né si registrano episodi pregressi ad ogni modo periodicamente la sede comunale a soggetta a controllo periodico da parte di soggetto qualificato.

La probabilità di verificazione dell'evento è perciò al momento stimata "bassa".

Relativamente alle misure adottate per la gestione degli impianti di sicurezza dei Data Center e ridurre il rischio di perdita dei dati del Comune a seguito di eventi naturali e/o artificiali, si rimanda alla procedura trattamento dei dati con strumenti elettronici.

12. Formazione

1. Il programma di formazione ha lo scopo di rendere consapevoli i dipendenti delle problematiche inerenti la sicurezza e di responsabilizzarli sulle attività da eseguire. L'attività formativa interessa tutto il personale.
2. Il Settore a cui compete la gestione dei processi di formazione cura la formazione dei nuovi assunti.
3. Ogni Settore deve curare la formazione dei propri dipendenti avvalendosi, se lo ritiene opportuno, della formazione on line e della collaborazione dell'ufficio che si occupa dell'organizzazione dell'attività formativa.
4. I corsi saranno progettati in base alle diverse esigenze e; in generale, non potranno mancare riferimenti a:
   - normativa vigente;
   - definizione delle responsabilità;
   - elenco delle vulnerabilità al fine di acquisire maggiore consapevolezza dei rischi che si possono correre;
   - regole comportamentali che comprendono la gestione degli accessi (password);
   - regole comportamentali di riservatezza sia in orario di lavoro sia al di fuori dell'ambito lavorativo;
   - i possibili rischi: virus, intercettazioni, intrusioni, ecc..

13. Accesso alle sedi e uffici

1. L'apertura e la chiusura della sede e l'accesso agli uffici durante gli orari di apertura al pubblico è affidata al personale preposto.

   Al di fuori degli orari di apertura non è previsto nessun tipo di accesso se non in casi straordinari; in questo caso l'accesso alla sede sarà permesso con la supervisione del personale preposto che provvederà all'apertura e chiusura della sede e al controllo di eventuali accessi non autorizzati durante il periodo di apertura straordinario.

14. Registro delle attività del Titolare del trattamento

1. Il Registro delle attività di trattamento svolte dall'Ente reca almeno le seguenti informazioni, come previste dall'art. 30 RGPD:
    a) il nome ed i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento e del Responsabile della Protezione Dati;
    b) le finalità del trattamento;
    c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
    d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
    e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
    f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
    g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il registro è aggiornato tempestivamente in occasione della variazione dei trattamenti e comunque almeno una volta ogni 12 mesi
3. Il registro è in formato elettronico, facilmente accessibile a tutti i soggetti autorizzati alla sua redazione ed è fruibile direttamente, senza intermediazione, da parte del DPO e dell'autorità di controllo.

15. Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. Il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto (DPIA) quando il trattamento medesimo, considerati la natura, l'oggetto, il contesto e le finalità dello stesso nonché l'eventuale utilizzo di nuove tecnologie, presenta un rischio elevato per i diritti e le libertà delle persone fisiche.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti, o non soggetti, a valutazione come redatti e pubblicati dal Garante per la protezione dei dati personali ai sensi dell'art. 35 del RGPD.
3. La DPIA non è necessaria nei casi seguenti:
    a) se il trattamento non presenta un rischio elevato per i diritti e le libertà di persone fisiche;
    b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
    c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
    d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta;

e) se i trattamenti sono già stati oggetto di verifica preliminare da parte del Garante della Privacy o del RPD e che proseguono con le stesse modalità oggetto di tale verifica.

16. Violazione dei dati personali

1. La violazione dei dati personali o "data breach" è una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ente.
2. Il Titolare o l'Incaricato devono opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.
3. Il Titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto. Il Titolare del trattamento, a prescindere dalla notifica al Garante, documenta tutte le violazioni dei dati personali, secondo le modalità individuate dall'Ufficio Privacy. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.
4. Il Responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il Titolare in modo che possa attivarsi.
5. Le notifiche al Garante effettuate oltre il termine delle 72 ore devono contenere i motivi del ritardo.

Capo IV – Organizzazione interna

17. Competenza in materia di transizione digitale

1. Ai sensi dell'art.17 del CAD (Codice Amministrazione Digitale) è individuato nell'ente locale un Responsabile per la Transizione al Digitale (RTD) per l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo che, in ambito di protezione dati, fornisca il contributo nella valutazione degli aspetti tecnologici, relativamente all'impatto di questi sulle attività di trattamento, fatte salve le eventuali specifiche competenze attribuite alla medesima struttura dal Titolare.
2. Il Responsabile per transizione digitale svolge i seguenti compiti:
    a) realizzazione di una apposita base di dati contenente le caratteristiche dell'infrastruttura tecnologica hardware e software utilizzata dall'Ente per le attività di trattamento di dati;
    b) sviluppo degli aspetti tecnologici inerenti all'analisi del rischio (ai sensi dell'art. 32 RGPD) e della valutazione di impatto (ai sensi dell'art. 35 RGPD);
    c) supporto alle Strutture organizzative nel caso di istanze degli Interessati che richiedano valutazioni di natura tecnologica relative agli strumenti di trattamento dati utilizzati dal Titolare;
    d) predisposizione della procedura interna di segnalazione data breach, nel caso di una violazione che abbia avuto ad oggetto sistemi tecnologici del Titolare del Trattamento o dei Responsabili del Trattamento

18. Rinvio

1. Per tutto quanto non espressamente disciplinato, si applicano le disposizioni del RGPD e tutte le norme vigenti in materia.