Comune di Pescara

Regolamento per la gestione e protezione dei dati personali e particolari

Delibera di C.C. n. 49 del 24.05.2018

Modificato integralmente con Delibera Di C.C. n. 10 del 20.01.2021

Sommario

CAPO I – OGGETTO E FINALITÀ

Art. 1 - Oggetto del regolamento

1. 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, di seguito indicato, con "GDPR"), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Pescara.

Art. 2 – Finalità del regolamento

1. Il Comune di Pescara, nell'assolvimento delle proprie finalità istituzionali secondo i principi di trasparenza, efficacia ed economicità sanciti dalla legislazione vigente, garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il rispetto del diritto degli individui all'autodeterminazione informata come definito dalla convenzione europea 108/1981.
2. In adempimento dell'obbligo di comunicazione interna ed esterna e di semplificazione dell'azione amministrativa, la finalità del presente regolamento è di favorire la trasmissione di dati e documenti tra le banche dati e gli archivi del Comune di Pescara, degli enti territoriali, degli enti pubblici, dei gestori e degli incaricati di pubblico servizio, operanti nell'ambito dell'Unione Europea.
3. La trasmissione dei dati può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità.
4. Ai fini del presente regolamento, per finalità istituzionali del Comune di Pescara si intendono le funzioni ad esso attribuite dalle leggi, dallo statuto e dai regolamenti, anche svolte per mezzo di intese, accordi, convenzioni.

CAPO II – FINALITÀ DEL TRATTAMENTO

Art. 3 – Finalità del Trattamento

1. I trattamenti dei dati personali sono compiuti dal Comune per le seguenti finalità:
   a) L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri in relazione a funzioni e compiti attribuiti o delegati. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
   b) L'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
   c) L'esecuzione di un contratto con soggetti interessati;
   d) Per finalità diverse da quelle di cui alle precedenti lettere, purché l'interessato esprima il consenso al trattamento.
2. I trattamenti effettuati devono avvenire in maniera lecita e corretta.

3. I trattamenti delle categorie particolari (ex sensibili) e giudiziari, necessari per **motivi di interesse pubblico rilevante** sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

CAPO III – SOGGETTI DEL TRATTAMENTO DEI DATI PERSONALI

Art. 4 – Titolare del Trattamento

1. Il Comune di Pescara, rappresentato ai fini previsti dal GDPR dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco può designare i Dirigenti dell'Ente, con proprio provvedimento ai sensi dell'art. 29 GDPR ed art. 2-quaterdecies D.lgs. 196/03 come modificato dal D.lgs. 101/18, per lo svolgimento di compiti e funzioni, per quanto di competenza dell'Ufficio di appartenenza (funzioni monocratiche con potere di firma, atti di designazione degli autorizzati al trattamento, accordi ex art. 26 e art. 28 GDPR).
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, 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 GDPR; le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
4. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione finanziaria generale dell'Ente DUP (Documento Unico di Programmazione), di Bilancio e di PEG (Piano Esecutivo di Gestione), previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di 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 adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

6. Nel caso in cui un tipo di trattamento, anche per l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con l'acronimo "DPIA" Data Protection Impact Analysis) ai sensi dell'art. 35 GDPR.

7. Il Titolare, sulla base del proprio ordinamento:

- Nomina ai sensi dell'art. 37 GDPR, con proprio specifico atto, il Responsabile della Protezione dei Dati (di seguito RPD/DPO Data Protection Officer);
- Individua uno o più Amministratori di Sistema.

Art. 5 – Dirigenti Designati/Dipendenti Autorizzati

1. Ai Dirigenti designati sono attribuiti compiti e funzioni connessi al trattamento dei dati personali nell'ambito dell'articolazione organizzativa di rispettiva competenza (Settore) per lo svolgimento dei quali possono avvalersi della collaborazione e consulenza del RPD-DPO.

2. Il Dirigente designato provvede, per il proprio ambito di competenza a tutte le attività previste dalla legge e a tutti i compiti affidati dal Titolare (ex art. 29 GDPR e art. 2 - quaterdecies D.lgs. 196/06 come modificato dal D.Lgs. 101/18) e in particolare :

- all'adozione di idonee misure tecniche ed organizzative adeguate per garantire la sicurezza dei trattamenti con il supporto del RPD/DPO, come da art. 32 GDPR e da valutazione di impatto ex art. 35 GDPR;
- alla compilazione e aggiornamento delle schede di propria rispettiva competenza del Registro dell'attività di Trattamento;
- alla designazione degli Autorizzati al Trattamento dei dati personali, ai sensi dell'art. 29 GDPR e art. 2-quaterdecies D.Lgs. 196/03 come modificato dal D.Lgs. 101/18, fornendo loro specifiche istruzioni;
- alla sensibilizzazione del personale autorizzato al trattamento dei dati personali e alle connesse attività di controllo favorendone la formazione;
- alla individuazione di uno o più Referenti Privacy per ogni Servizio in ragione della sua complessità, con il compito di supportare gli autorizzati al trattamento dei dati personali, sia a livello informativo che operativo;
- alla individuazione, contrattualizzazione e nomina dei Responsabili di Trattamento esterni, nel rispetto dell'art. 28 GDPR, nonché alla sottoscrizione di accordi - mediante atto giuridico vincolante con la persona fisica, giuridica, pubblica amministrazione o ente (Responsabile del Trattamento) che tratta i dati per conto del Titolare del trattamento - nei quali siano impartiti istruzioni, facoltà e doveri dei Responsabili nei confronti del Titolare;

- alla stipula dell'accordo di contitolarità, di cui all'art. 26 GDPR, qualora il trattamento venga effettuato congiuntamente ad un altro Titolare del trattamento, determinando congiuntamente le finalità ed i mezzi del trattamento stesso;
- alla definizione per gli Interessati delle specifiche informative sul trattamento dei dati personali, secondo gli artt. 13 e 14 GDPR, provvedendo a renderle costantemente aggiornate e facilmente accessibili, mediante la consulenza del Responsabile Protezione Dati (RPD/DPO);
- alla evasione delle istanze degli interessati comprese quelle relative all'esercizio del diritto di accesso;
- alla collaborazione con il Dirigente del Settore cui è ascritta la competenza in materia di protezione dei dati, in ordine al monitoraggio dell'andamento delle attività di trattamento dati realizzato attraverso questionari di autovalutazione, attività di Audit interno, reclami e violazioni;
- alla valutazione dei rischi sulla protezione dei dati personali (DPIA) di concerto con il RPD/DPO e i rispettivi Referenti Privacy individuati ai fini della stesura del DPIA stesso;
- alla gestione dei casi di violazione dei dati personali (DATA BREACH) secondo le procedure definite.

Art. 6- Dirigente competente in materia di protezione dei dati

1. Il Dirigente competente in materia di protezione dei dati coordina il funzionamento del "sistema" della protezione dei dati dell'Ente avvalendosi della propria Struttura, dei Dirigenti designati, dei Referenti Privacy e della collaborazione del RPD/DPO. In particolare, con il supporto tecnico del RPD/DPO, provvede:

- alla predisposizione delle proposte di provvedimenti da adottarsi in materia, da parte del Sindaco, della Giunta e del Consiglio Comunale;
- al monitoraggio dell'andamento delle attività in materia di protezione dei dati attraverso questionari di autovalutazione, attività di audit interno, gestione reclami, violazioni;
- a sovrintendere all'aggiornamento del Registro delle attività di Trattamento su istanza del Dirigente designato, di volta in volta competente. La compilazione e l'aggiornamento periodico delle schede del Registro del trattamento dovrà avvenire almeno una volta per anno solare coordinata dal RPD/DPO ed eseguita da ciascun Dirigente designato responsabile dei Servizi a cui i dati afferiscono per le parti di propria competenza.

Art. 7 – Competenze del Referente Privacy

1. Il Referente Privacy adempie ai seguenti compiti:

a) coadiuvare i dirigenti nella predisposizione degli atti per identificare e designare, per iscritto e in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la

struttura organizzativa di competenza, le persone fisiche della struttura organizzativa medesima, che operano sotto la diretta autorità del Titolare, e attribuire alle persone medesime specifici compiti e funzioni inerenti al trattamento dei dati;

b) coadiuvare gli uffici come punto di contatto con il RPD-DPO;
c) coadiuvare i dirigenti nella ricognizione di tutti i trattamenti di dati personali, sensibili e giudiziari svolti nella struttura organizzativa di competenza, in correlazione con i processi/procedimenti svolti dall'Ufficio, da sottoporre all'approvazione del Titolare;
d) coadiuvare i dirigenti ad effettuare l'analisi del rischio dei trattamenti, e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli interessati, da sottoporre all'approvazione del Titolare;
e) coadiuvare i dirigenti ad effettuare prima di procedere al trattamento, quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, una valutazione dell'impatto del trattamento sulla protezione dei dati personali;
f) in caso di violazione dei dati personali, collaborare con il Dirigente, il RPD-DPO per notificare la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;
g) coadiuvare i dirigenti affinché il RPD-DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
h) coadiuvare i dirigenti a sostenere il RPD-DPO nell'esecuzione dei propri compiti fornendogli le informazioni e documenti necessari per assolvere gli stessi e accedere ai dati personali e ai trattamenti;
i) coadiuvare i dirigenti ad attuare la formazione in tema di diritti e libertà degli interessati, di rischi di violazione dei dati, di informatica giuridica, e di diritto;
j) coadiuvare i dirigenti a promuovere la cultura della prevenzione del rischio di violazione dei dati e la cultura della protezione dei dati come valore da integrare in ogni processo/procedimento;
k) coadiuvare i dirigenti ad effettuare ogni ulteriore attività, non espressamente indicata in precedenza e necessaria per la integrale attuazione del GDPR e della normativa interna di adeguamento;
l) coadiuvare il RPD-DPO nello svolgimento delle proprie funzioni.

Art. 8 – Amministratore di Sistema

1. Il Titolare, nella persona del Sindaco rappresentante pro tempore dell'Ente, individua gli Amministratori di Sistema tra i dipendenti assegnati al Servizio CED dell'Ente.
2. La nomina di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. La designazione dell'amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
3. L'amministratore di sistema svolge attività, quali: il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware e propone al Titolare, di concerto con il Responsabile della Transizione Digitale un documento di valutazione del rischio informatico.
4. Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste; devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore a sei mesi.
5. L'Amministratore di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

Art. 9 – Contitolarità del trattamento

1. Il Regolamento UE 679/2016 disciplina con l'art. 26 l'ipotesi in cui il trattamento dei dati personali può essere effettuato da uno o più titolari.
2. Nel caso in cui si determini una situazione di "contitolarità" del trattamento e cioè quando "due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento" è necessario prevedere un accordo scritto, stipulato dal Dirigente designato competente per materia, con il quale si disciplinano le responsabilità, il rispetto degli obblighi previsti dal Regolamento UE 679/2016 e i ruoli.
3. Gli accordi di contitolarità dovranno indicare in maniera trasparente le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento UE 679/2016, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del

trattamento sono soggetti. Tale accordo deve prevedere espressamente la modalità con cui gli interessati possano far valer i propri diritti o richiedere informazioni.

4. L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

5. Indipendentemente dalle disposizioni dell'accordo interno, l'interessato può esercitare i propri diritti nei confronti di ciascun Titolare del trattamento.

Art. 10 – Responsabile del Trattamento

1. Il Titolare, nella persona del Dirigente designato, competente per materia, può prevedere ai sensi dell'art. 28 GDPR, l'esternalizzazione totale o parziale di un trattamento di dati personali mediante contratto o altro atto giuridico.

2. Questa fattispecie non implica alcuna deresponsabilizzazione per l'Ente che dovrà verificare la conformità normativa delle attività di trattamento esternalizzate.

3. Nel caso di esternalizzazione del trattamento di dati personali è necessario formalizzare in maniera scritta gli obblighi delle parti preposte alle attività di trattamento, definendone modalità, condizioni, durata, natura e finalità e chiarendo espressamente il tipo di dati personali trattati, le categorie di interessati, nonché gli obblighi e i diritti del Titolare del trattamento e del responsabile del trattamento designato.

4. La designazione formale è necessaria sia nel caso in cui il Titolare affidi uno specifico trattamento a un responsabile sia qualora un responsabile del trattamento affidi a un altro responsabile del trattamento (sub-responsabile) l'esecuzione di specifiche attività di trattamento per conto del Titolare.

5. Gli accordi, che possono avere solo la forma scritta (anche formato elettronico) e con atto vincolante per il responsabile del trattamento, devono prevedere: l'obbligo di trattare i dati solo in conformità alle istruzioni ricevute dal Titolare; l'obbligo di garantire che le persone fisiche autorizzate alle attività di trattamento siano vincolate da obblighi di riservatezza, contrattualmente assunti o stabiliti per legge; l'obbligo di adottare le misure richieste ai sensi dell'art. 32 del Regolamento, vale a dire le misure tecniche e organizzative a protezione dei dati ritenuti idonee a garantire un livello di sicurezza adeguato al rischio insito nel trattamento; l'imposizione degli stessi obblighi verso l'eventuale sub-responsabile; l'obbligo di assistere il Titolare, mediante misure tecniche e organizzative adeguate, nel dar seguito alle eventuali richieste degli interessati (accesso, rettifica, cancellazione, portabilità, opposizione); le attività di notifica di eventuali data breach.

Art. 11 – Responsabile della Protezione dei Dati (RPD)/Data Protection Officer (DPO)

1. Il Comune si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD/DPO), in possesso delle qualità professionali, in particolare della conoscenza specialistica

della normativa e delle prassi in materia di protezione dei dati, e della capacità tecnica specialistica di assolvere i connessi compiti.

2. Il Comune non può procedere nella sua attività istituzionale senza un Responsabile della Protezione (RPD-DPO) secondo l'art. 37 del GDPR con le funzioni, compiti e responsabilità previsti dal Regolamento Europeo e normativa nazionale.

3. Il RPD-DPO può essere un dipendente in posizione apicale oppure un incaricato individuato previo espletamento di procedura ad evidenza pubblica.

4. Nel caso di RPD-DPO individuato a seguito di procedura ad evidenza pubblica, la designazione dello stesso avviene con decreto del Sindaco rappresentante pro tempore dell'Ente, a seguito di determina di aggiudicazione ai sensi del D.Lgs n. 50/2016.

5. La figura del DPO è incompatibile con chi determina le finalità o i mezzi del trattamento. In particolare, risultano con la stessa incompatibili:

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

6. Sul sito istituzionale vanno pubblicati i dati di contatto del RPD-DPO. Gli stessi vanno comunicati al Garante della protezione dei dati personali.

7. Il RPD-DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, deve avere la possibilità di accedere ai dati personali e ai trattamenti.

8. Gli interessati possono contattare il RPD-DPO per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

9. Il RPD-DPO è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti, in conformità al diritto dell'Unione o degli Stati membri deve svolgere almeno le seguenti funzioni:

a) informare e fornire consulenza al Sindaco, ai Dirigenti, agli organi collegiali e a tutti gli uffici in merito agli obblighi derivanti dal presente regolamento nonché dalla normativa nazionale e comunitaria;

b) sorvegliare l'osservanza del presente regolamento nonché della normativa nazionale e comunitaria da parte dei titolari del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire supporto tecnico e specialistico ai Dirigenti designati in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento (DPIA);

d) supportare il Dirigente competente in materia di Privacy circa l'attività di monitoraggio dell'andamento delle attività in materia di protezione dei dati personali attraverso questionari di autovalutazione, attività di Audit interno, gestione di reclami, violazioni;

e) in sede di Audit, esprimere rilievi, prescrizioni e raccomandazioni;

f) redigere un Piano di Protezione dei Dati e di Gestione del Rischio di violazione (PRG) secondo le disposizioni del GDPR provvedendo altresì a definire le procedure per la gestione dei reclami, quelle di risposta agli incidenti di sicurezza nonché la tipologia di comunicazione da trasmettere, in caso di Data Breach, ai soggetti interessati e all'Autorità;

g) provvedere alla verifica della corretta tenuta del Registro dell'attività di trattamento;

h) cooperare con l'Autorità garante per la protezione dei dati personali costituendo il punto di contatto per le questioni connesse al trattamento dei dati personali.

10. Il RPD-DPO è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione con onere di comunicazione di detto adempimento al Titolare del trattamento.

11. Il Titolare ed il Responsabile del trattamento assicurano che il RPD-DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

a. il RPD-DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti che abbiano per oggetto questioni inerenti la protezione dei dati personali;
b. il RPD-DPO deve ricevere tempestivamente tramite posta elettronica, dai Dirigenti designati e dal Responsabile del trattamento dati tutte le informazioni pertinenti le decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea;
c. il RPD-DPO viene consultato obbligatoriamente sugli aspetti riguardanti la sicurezza dei trattamenti e la liceità degli stessi prima di pubblicare bandi di gara e avvisi che hanno impatto sulla protezione dei dati personali;
d. il RPD-DPO deve essere consultato obbligatoriamente nella predisposizione o adeguamento dei regolamenti che impattano sulla protezione dei dati personali;
e. il parere del RPD-DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD-DPO, è necessario motivare specificamente tale decisione;
f. il RPD-DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente (Data Breach); con proprio parere indica quali provvedimenti debbano essere adottati per porre rimedio ovvero per prevenire il ripetersi di tali violazioni.

12. Nello svolgimento dei compiti affidatigli il RPD-DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD-DPO:

- Procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati avvalendosi della collaborazione dei Dirigenti designati e dei Responsabili del trattamento dati interessati nell'area di mappatura;
- Definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

13. Il RPD-DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione di una specifica questione attinente alla normativa in materia di protezione dei dati. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD-DPO riferisce direttamente al Titolare. Non può essere rimosso o penalizzato dal Titolare in ragione dell'adempimento dei propri compiti. Nel caso in cui rilevi o siano sottoposte alla sua attenzione decisioni incompatibili con il GDPR o con le indicazioni dallo stesso RPD-DPO fornite, è tenuto a manifestare il proprio dissenso comunicandolo al Titolare.

14. Il RPD-DPO si avvale dei "referenti privacy", designati dai Dirigenti.

CAPO IV – TRATTAMENTO DEI DATI PERSONALI

Art. 12 - Attività amministrativa

1. L'attività amministrativa del Comune si svolge, principalmente, con l'emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.

2. Per l'attività amministrativa di cui al comma precedente sono rigorosamente rispettate le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Ente.

3. Per l'attività di cui al comma precedente sono rigorosamente rispettate le norme di cui al codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni e le istruzioni operative all'utilizzo dei sistemi informatici allegato a questo regolamento.

4. La gestione dei documenti informatici contenenti dati personali è soggetta alla specifica disciplina prevista dal GDPR 679/2016 e del D.Lgs n. 196/2003 e al regolamento di gestione dei documenti informatici.

5. La sicurezza dei dati personali contenuti nei documenti di cui al comma precedente è assicurata anche mediante adeguate soluzioni tecniche connesse all'utilizzo della firma digitale,

chiavi biometriche o altre soluzioni tecniche idonee al trattamento dei dati personali e sensibili come pseudonimizzazione, criptazione dei dati e minimizzazione.

Art. 13 – Principi del trattamento

1. Il GDPR delinea all'art. 5 sei principi che l'Ente deve rispettare quando raccoglie, tratta e memorizza i dati personali:

- Liceità, Correttezza e Trasparenza: l'Ente deve assicurarsi che l'attività di raccolta dei dati personali degli utenti non infranga la legge e che non nasconda nulla agli interessati. A tale scopo, è necessario mettere a disposizione del pubblico l'informativa sulla privacy, ossia un documento che spieghi in maniera chiara, concisa ma completa le finalità della raccolta dei dati e come si intenda usarli;
- Limitazione della finalità: l'Ente deve raccogliere i dati personali solamente per uno scopo preciso che, peraltro, va indicato in modo chiaro nell'Informativa sulla Privacy; inoltre, tali dati vanno tenuti solo per il tempo necessario a completare lo scopo per cui sono stati raccolti;
- Minimizzazione dei dati: l'ente può elaborare solo i dati personali necessari al raggiungimento della finalità per i quali sono trattati;
- Esattezza: l'accuratezza dei dati personali è parte integrante della loro protezione. Il GDPR afferma che "devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti". Gli interessati hanno il diritto di chiedere che i propri dati personali inesatti o incompleti vengano cancellati o rettificati (Articoli 16 e 17);
- Limitazione della conservazione: l'Ente deve eliminare i dati personali quando non sono più necessari ai propri scopi;
- Integrità e riservatezza: il GDPR afferma che i dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali".

Art. 14 - Categorie di dati e modalità di trattamento

1. Ai sensi degli articoli 4, 9 e 10 GDPR, il trattamento riguarda le seguenti categorie di dati:

- Dati personali comuni: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere individuata direttamente o indirettamente con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, fisica, economica, culturale o sociale;
- Dati particolari: qualsiasi dato personale che riveli l'origine razziale o etnica, le opinioni

politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale nonché dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

- Dati relativi a condanne penali o reati;

2. Il trattamento si svolge nel rispetto dei principi stabiliti dall'art. 5 del GDPR e dei diritti dell'interessato previsti nel capo terzo del GDPR. Il trattamento dei dati particolari e dei dati relativi a condanne penali e reati è meglio dettagliato nel successivo art. 15.

3. Ai sensi dell'art. 12 del GDPR il Titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 (dati personali raccolti presso l'interessato) e 14 (dati personali raccolti non direttamente presso l'interessato) relative al trattamento. L'informativa che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile, deve contenere gli elementi tassativamente indicati rispettivamente agli artt. 13 e 14 e deve essere data, in linea di principio, per iscritto, in formato elettronico o altrimenti nel rispetto di quanto previsto dal regolamento UE.

Art. 15 - Trattamento dei dati particolari e dei dati relativi a condanne penali e reati

1. E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, fatti salvi i casi di cui al comma 2.

2. Il Titolare tratta tali dati se si verifica uno dei seguenti casi:

- se l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche;
- per diritti dell'interessato in materia di diritto del lavoro, sicurezza sociale e protezione sociale, in base a norma di legge o contratto collettivo;
- per un interesse vitale dell'interessato o di altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- se il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione europea e degli stati membri ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, da regolamenti che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
- se il trattamento è necessario ai fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici ed è proporzionato alla finalità perseguita.

3. I dati particolari e i dati relativi a condanne penali e a reati sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi,

soprattutto nel caso in cui la raccolta non avvenga presso l'interessato.

4. I dati particolari e i dati relativi a condanne penali e a reati, non indispensabili, dei quali il Titolare, nell'espletamento della propria attività istituzionale, venga a conoscenza, ad opera dell'interessato, comunque, non a richiesta del Comune medesimo, non sono utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

5. Nei casi indicati vanno sempre previste misure di garanzia appropriate e specifiche per tutelare i diritti fondamentali e gli interessati.

Art. 16 – Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

1. Il Titolare, in sede di pubblicazione e diffusione, tramite l'Albo pretorio informatico, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:

a. sicurezza
b. completezza
c. esattezza
d. accessibilità
e. legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità
f. rispetto delle finalità perseguite.

2. Negli atti destinati alla pubblicazione o divulgazione i dati che permettono di identificare gli interessati sono riportati solo quando è necessario ed è previsto da una norma di legge o, nei casi previsti da legge, da regolamenti.

3. I sistemi informativi ed i programmi informatici devono essere configurati per ridurre al minimo l'utilizzazione di dati personali e devono prevedere la possibilità di estrazione degli atti, con l'esclusione dei dati personali in essi contenuti.

4. Qualora gli atti e i documenti resi conoscibili o pubblici debbano contenere dati di carattere personale, al fine di rispettare il principio di pubblicità dell'attività amministrativa, deve essere rispettato il principio di proporzionalità, verificando se sono pertinenti e non eccedenti rispetto alle finalità perseguite.

5. Salva diversa disposizione di legge, il Titolare garantisce la riservatezza dei dati particolari in sede di pubblicazione sull'Albo on line, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il Titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.

6. In ogni caso, i documenti, soggetti a pubblicazione, riportanti informazioni di carattere

particolare e/o relative a condanne penali e a reati, devono essere anonimizzati con adeguate tecniche come quelle previste dall'art. 32 del GDPR.

7. I dati particolari e quelli relativi a condanne penali e a reati sono sottratti all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo.

Art. 17 - Pubblicazione web per obblighi di trasparenza

1. Il Titolare effettua il trattamento di dati personali, contenuti in atti e documenti amministrativi, che devono essere pubblicati sul web per obblighi di trasparenza previsti dal D.lgs. n. 33/2013 e ss.mm.ii.

2. I documenti di cui al comma 1 sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione e costantemente aggiornati.

3. Laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, tranne deroghe previste da specifiche disposizioni.

4. Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.

5. I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati particolari relativi alla vita sessuale non possono essere diffusi per finalità di trasparenza.

6. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.

7. I dati vanno pubblicati in formato di tipo aperto, ai sensi dell'art. 68, D.lgs. n. 82/2005. I dati personali diversi dai dati particolari e dai dati relativi a condanne penali e reati, possono essere diffusi attraverso siti istituzionali, nonché trattati secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web.

8. I dati, le informazioni e i documenti di cui al comma 1, sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello dell'obbligo di pubblicazione.

9. Deroghe alla predetta durata temporale quinquennale sono previste:

a) nel caso in cui gli atti producano ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;
b) per alcuni dati e informazioni riguardanti i titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale ai sensi dell'art. 14, comma 2, D.Lgs n. 33/2013 e i titolari di incarichi dirigenziali e di collaborazione o consulenza che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell'incarico ai sensi dell'art. 15, comma 4, D.Lgs n. 33/2013;

c) nel caso in cui siano previsti diversi termini dalla normativa in materia di trattamento dei dati personali.

10. I dati personali devono essere conservati, in ogni caso, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati; l'interessato ha sempre diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.

Art. 18 – Pertinenza delle informazioni contenenti dati personali ai fini dell'accesso e della trasparenza

1. Il Titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

2. I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico e dal relativo Regolamento Comunale sull'Accesso.

3. Non possono essere disposti filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente".

4. Qualora i dati personali contenuti nei documenti non siano pertinenti o siano eccedenti rispetto all'interesse manifestato dal richiedente nell'istanza di ostensione, al fine di salvaguardare la riservatezza di terzi, l'accesso agli atti può essere limitato, su valutazione del Dirigente/ Responsabile del procedimento, mediante l'adozione di misure di sicurezza adeguate, compresa la pseudonimizzazione, la minimizzazione, la cifratura dei dati personali e l'occultamento.

5. Il Dirigente /Responsabile del Procedimento destinatari dell'istanza di accesso possono consultare il RPD/DPO, al fine di garantire la massima protezione dei dati personali.

Art. 19 - Registro del trattamento

1. In attuazione del Regolamento UE 679/2016 è istituito il Registro delle attività di trattamento che identifica l'elenco delle attività di trattamento effettuate dall'Ente, i tipi di dati particolari e dati relativi a condanne penali e reati per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite (art. 30 del Regolamento UE 679/2016);

2. La compilazione e l'aggiornamento del Registro, a cadenza annuale, è curato dai Dirigenti, ciascuno per rispettiva competenza, con il supporto del RPD/DPO e dei Referenti Privacy.

3. Il RPD/DPO in caso di indicazioni cogenti del Garante della Privacy, dell'AGID o di altri organismi competenti, coordina l'attività degli uffici, al fine di aggiornare e modificare, secondo

dette indicazioni, il registro di cui al comma precedente.

4. Il Registro, su supporto cartaceo o in formato digitale, detenuto dal RPD/DPO, deve essere approvato con Deliberazione di Giunta Comunale.

5. Il Registro delle attività di trattamento, in quanto norma di organizzazione dell'Ente, costituisce anche una forma di autorizzazione al trattamento dei dati personali da parte dei soggetti appartenenti alla struttura comunale, in quanto autorizzati al trattamento dei dati di competenza del Settore di riferimento, sulla base di quanto previsto dall'art. 2-quaterdecies del D.Lgs. 30 giugno 2003, n. 196.

6. Il Registro contiene le seguenti informazioni:

- dati di contatto del Titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- finalità del trattamento, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

7. Anche i Responsabili del trattamento, che svolgono tali attività per conto del Comune di Pescara, sono obbligati a tenere e ad aggiornare analogo Registro.

8. Su richiesta, il Comune di Pescara o il Responsabile del trattamento, mettono il registro a disposizione del Garante.

Art. 20. Fascicolo personale dipendenti e amministratori

1. I dati sullo stato di salute dei dipendenti e degli amministratori devono essere conservati separatamente rispetto alle altre informazioni personali. Il fascicolo, che raccoglie tutti gli atti relativi al loro percorso professionale e ai fatti più significativi che li riguardano, può mantenere la loro unitarietà, adottando accorgimenti che impediscano un accesso indiscriminato, quali l'utilizzo di sezioni o fascicoli dedicati alla custodia di eventuali dati particolari, da conservare chiusi o comunque con modalità che riducano la possibilità di una indistinta consultazione nel corso delle ordinarie attività amministrative.

Art. 21 - Formazione del personale

1. L'Ente deve garantire, con l'intervento del RPD/DPO, adeguata formazione al personale al fine di assicurare, nello svolgimento dell'attività degli uffici, il massimo livello di trasparenza possibile e l'assoluto rispetto dei diritti di riservatezza dei dati personali dei cittadini e dipendenti**.**

2. La partecipazione del personale dipendente agli interventi formativi è considerata quale elemento di misurazione e valutazione della *performance* organizzativa ed individuale.

CAPO V - DIRITTI DELL' INTERESSATO

Art. 22 – Diritti dell'interessato

1. Il Titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, in conformità alla disciplina contenuta nel GDPR e nel Codice.

2. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di accesso, secondo la quale, l'interessato ha il diritto di ottenere dal Comune di Pescara la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a. le finalità del trattamento;
b. le categorie di dati personali in questione;
c. i destinatari a cui i dati personali sono comunicati e qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate;
d. il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e. l'esistenza del proprio diritto a richiedere la rettifica o cancellazione del dato o la limitazione dei dati o di opporsi al loro trattamento;
f. il diritto di proporre reclamo a un'autorità di controllo;
g. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h. l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. La richiesta va inoltrata in forma scritta dall'interessato senza particolari formalità; in caso sia inoltrata con mezzi elettronici, salvo contraria indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.

4. Il Titolare deve fornire risposta entro 30 giorni dal ricevimento della richiesta, termine che può essere prorogato di due mesi in casi di particolari complessità o ricorra un giustificato motivo, avvisando l'interessato del differimento, entro un mese dall'istanza.

5. L'accesso dell'interessato ai propri dati personali può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo

svolgimento di indagini o per salvaguardare esigenze di riservatezza del Titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.

6. I diritti degli interessati possono essere ritardati, limitati o esclusi solo quando lo prevede una disposizione di legge e nel dettaglio:
   a. per non compromettere il buon esito dell'attività' di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, nonché l'applicazione delle misure di prevenzione personali e patrimoniali e delle misure di sicurezza;
   b. per tutelare la sicurezza pubblica;
   c. per tutelare la sicurezza nazionale;
   d. per tutelare i diritti e la libertà altrui;
   e. quando è impossibile o è necessario uno sforzo spropositato;
   f. per una previsione normativa espressa;
   g. tutela del segreto.
7. I soggetti di cui al capo III del presente regolamento sono tenuti a collaborare per la verifica della sussistenza del diritto anche chiedendo informazioni all'interessato, per consentire l'esercizio del diritto.

Art. 23 – Modalità di esercizio dei diritti dell'interessato

1. In qualunque momento i cittadini possono far valere i diritti previsti dal regolamento generale sulla protezione dei dati 679/2016 dagli artt. 15 e successivi.
2. Al fine di facilitare l'esercizio dei diritti dell'interessato in materia di protezione dati personali si rende disponibile il modulo per l'accesso ai dati personali che viene pubblicato sul sito istituzionale nella sezione Amministrazione trasparente e nella sezione privacy.

Art. 24 - Obbligo di informativa

1. Prima che inizi qualunque trattamento di dati personali il Titolare fornisce all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti.
2. L'informativa sul trattamento dei dati personali deve essere fornita per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.
3. Essa va effettuata:
   a. in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, nel momento della raccolta dei dati;
   b. in caso di dati personali non ottenuti presso l'interessato:
      - entro un termine ragionevole, massimo di un mese dalla raccolta (non registrazione) dei dati;

- nel caso in cui i dati vadano comunicati all'interessato alla prima comunicazione;
- se i dati personali devono essere comunicati ad un altro destinatario, non oltre la prima comunicazione.

4. Non è necessario fornire l'informativa:
   a. nel caso in cui l'interessato disponga già di tutte le informazioni necessarie;
   b. nel caso in cui la comunicazione risulti impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi il Titolare del trattamento adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con pubbliche informazioni.

CAPO VI – MISURE DI SICUREZZA

Art. 25 - Sicurezza dei dati – Misure di sicurezza

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, il Titolare del trattamento mette in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, che comprendono:
   - la pseudonimizzazione;
   - la minimizzazione;
   - la cifratura dei dati personali;
   - la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
   - la capacità di ripristinare tempestivamente la disponibilità e accesso dei dati in caso di incidente fisico o tecnico;
   - una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.
2. Costituiscono misure tecniche ed organizzative che possono essere adottate:
   - sistemi di autenticazione;
   - sistemi di autorizzazione;
   - sistemi di protezione (antivirus, firewall, antintrusione altro);
   - misure antincendio;
   - sistemi di rilevazione di intrusione;
   - sistemi di sorveglianza;
   - sistemi di protezione con videosorveglianza;
   - registrazione accessi;

- porte, armadi e contenitori dotati di serrature e ignifughi;
- 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.

3. Sarà necessario stipulare un contratto con una società terza, scelta in base alle proprie competenze professionali, per una valutazione periodica della sicurezza delle 'applicazioni web' e delle reti informatiche, di conseguenza i test riguarderanno tutto il sistema informatico. Il contratto di chi effettua il pen test, deve presentare clausole di riservatezza, gli indirizzi IP da cui partiranno i test, le persone fisiche responsabili e operative durante l'attività, e l'eventuale collaborazione con operatori e amministratori interni. Colui che effettua un pen test di un sistema deve garantire la non interruzione delle attività e processi, la non modifica e perdita dei dati e informazioni. Tutte le attività non regolamentate dal contratto sono considerate illegali.

4. L'ente e ciascun Dirigente designato si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca sotto la loro autorità ed abbia accesso ai dati personali.

5. I nominativi e i dati di contatto del Titolare e del responsabile della Protezione dei Dati (RPD-DPO) sono pubblicati sul sito istituzionale del Comune.

Art. 26 – Piano di Protezione dei dati personali e gestione del rischio di violazione

1. Sul presupposto del principio della responsabilizzazione del Titolare e del Responsabile del trattamento (accountability) l'Ente si dota di un Piano di Protezione dei Dati (PPD) idoneo a prevenire trattamenti illeciti e violazioni attribuibili a vulnerabilità della sicurezza.

2. Il piano di protezione dei dati personali e gestione del rischio di violazione da redigere e da aggiornare periodicamente su impulso del DPO, descrive le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche/logiche, logistiche/fisiche, organizzative e procedurali da adottare e da applicare per ridurre/eliminare il rischio di violazione dei dati derivante dal trattamento.

Art. 27 – Valutazione di impatto sulla protezione dei dati personali (DPIA)

1. Il Titolare, quando la tipologia di trattamento, definita nel registro delle attività di trattamento, "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1 GDPR), prima di effettuare il trattamento, deve attuare una valutazione di impatto del trattamento previsto sulla protezione dei dati personali (DPIA).

2. La valutazione d'impatto sulla protezione dei dati personali DPIA, è effettuata dai Dirigenti su impulso del RPD-DPO secondo quanto previsto dall'art. 35 GDPR e tenuto conto dei

provvedimenti del Garante relativi agli elenchi delle tipologie di trattamenti soggetti alla valutazione d'impatto.

3. Il DPIA conterrà quanto definito all'articolo 35, paragrafo 7, come segue:
   a) una **descrizione sistematica dei trattamenti previsti** e delle **finalità** del trattamento, compreso, ove applicabile, **l'interesse legittimo** perseguito dal Titolare del trattamento;
   b) una **valutazione della necessità e proporzionalità** dei trattamenti in relazione alle finalità;
   c) una **valutazione dei rischi per i diritti e le libertà** degli interessati;
   d) le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento UE, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

4. I Dirigenti provvedono alla valutazione d'impatto su impulso del Responsabile della protezione dei dati il quale deve trasmette alle strutture Dirigenziali (Dirigenti/Referenti Privacy) processi documentati per la valutazione dei rischi sulla protezione dei dati personali anche in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi; deve fornire la necessaria consulenza per la redazione del DPIA; deve sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati.

5. Qualora il trattamento venga eseguito in toto o in parte da un Responsabile del trattamento dei dati, **quest'ultimo deve assistere il Titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati** e fornire tutte le informazioni necessarie.

6. La valutazione d'impatto è condotta prima di dar luogo al trattamento, attraverso i seguenti processi riportati nel DPIA:
   a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
   b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
      - delle finalità specifiche, esplicite e legittime;
      - della liceità del trattamento;
      - dei dati adeguati, pertinenti e limitati a quanto necessario;
      - del periodo limitato di conservazione;
      - delle informazioni fornite agli interessati;
      - del diritto di accesso e portabilità dei dati;
      - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;

- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

c) individuazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi stessi (Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio del trattamento dei dati personali; Es. Azioni non autorizzate, Compromissione informazioni, Problemi tecnici ed interruzione di servizi, Eventi naturali);

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

7. Ai sensi dell'art. 36 GDPR il Titolare del trattamento, prima di procedere al trattamento, consulta l'Autorità di Controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'art. 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare stesso per attenuare il rischio.

Art. 28 – Pubblicazione sintesi della valutazione d'impatto (D.P.I.A.)

1. Il Titolare effettua la pubblicazione del D.P.I.A. o di una sintesi dello stesso.

2. Il D.P.I.A. pubblicato non deve contenere l'intera valutazione, qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze o in una dichiarazione che attesti la realizzazione della stessa.

CAPO VII - DATA BREACH O VIOLAZIONE DEI DATI PERSONALI

Art. 29 – Notifica delle violazioni dei dati personali

1. Una violazione di dati personali (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 ai dati personali trasmessi, conservati o comunque trattati.

2. Le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni*:*

- "**violazione della riservatezza**", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "**violazione dell'integrità**", in caso di modifica non autorizzata o accidentale dei dati personali;
- "**violazione della disponibilità**", in caso di perdita, accesso o distruzione accidentali o non

autorizzati di dati personali.

3. I Principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie, danno economico o sociale;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Ogni violazione di dati personali deve essere documentata in un apposito registro di Data Breach approvato con Deliberazione di Giunta Comunale**.**

5. A norma dell'art. 33 GDPR, il Titolare del trattamento deve notificare la violazione all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, la stessa deve essere corredata dei motivi del ritardo.

6. il Titolare del trattamento (Dirigenti) deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio posto che tale documentazione consente all'autorità di controllo di verificare il rispetto della disciplina in tema di notifiche di violazioni.

7. Il Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

8. Se il Titolare del trattamento (Dirigente) ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare detti interessati senza ingiustificato ritardo. Sono considerati rischi elevati violazioni che, a titolo di esempio, possono:

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

CAPO VIII - DISPOSIZIONI FINALI

Art. 30 – Disposizioni finali

1. Per quanto non previsto nel presente Regolamento si applicano:
   - le disposizioni del GDPR;
   - le disposizioni del Codice Privacy;
   - le Linee guida e i provvedimenti del Garante;
   - i Regolamenti adottati dall'Ente per specifici ambiti (es. videosorveglianza)