CITTÀ DI CASSINO
Provincia di Frosinone
P.zza De Gasperi, 1 – 03043 - Cassino (FR)

Regolamento Comunale per l'attuazione

del Regolamento UE 2016/679

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Approvato con delibera di Consiglio Comunale n.55 del 2022

INDICE:

Art. 1
Oggetto

Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione dell'allegato Regolamento Europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", 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 Cassino e nei terzi che trattano dati per il Comune stesso.

Art.2
Titolare del trattamento e Contitolarità

1. Il Comune di Cassino (di seguito indicato con "*Titolare*"), ai fini previsti dal RGPD, è il "Titolare" del trattamento dei dati personali contenuti in archivi cartacei e digitali, già detenuti o destinati a figurarvi, interamente o parzialmente.
2. Il Sindaco *pro tempore* è il rappresentante del "Titolare".
3. Il "Titolare" è competente per il rispetto dei principi applicabili al trattamento dei dati personali di cui all'art. 5 RGDP, di cui, tra gli altri, i principi di liceità, correttezza e trasparenza.
4. Il "Titolare" mette in atto 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. Tali misure sono riesaminate e aggiornate se necessario ed attuate nell'ambito della programmazione operativa di cui al DUP, al PEG ed al bilancio.

   A tale scopo, il "Titolare":

   a. delega le relative funzioni al Dirigente/Responsabile Posizione Organizzativa di ciascuna Area, ai fini del trattamento dei dati del relativo settore, in possesso di adeguate competenze e autorizzato mediante apposito decreto sindacale, ai sensi dell'art. 4 del presente Regolamento, fermo restando la sua responsabilità nel trattamento dei dati personali ai sensi dell'art. 24 del RGPD;
   b. adotta le misure tecniche e organizzative, quali la pseudonimizzazione e la minimizzazione, fin dalla fase di progettazione (privacy by design) per garantire che siano trattati per impostazione predefinita (privacy by default) solo i dati necessari per ogni specifica finalità di trattamento;
   c. fornisce all'interessato in forma concisa, trasparente, intellegibile e facilmente accessibile con un linguaggio semplice e chiaro:
      - tutte le informazioni di cui all' art. 13 del RGPD qualora i dati personali siano raccolti presso lo stesso interessato;

- tutte le informazioni di cui all' art. 14 del RGPD qualora i dati personali non siano raccolti presso lo stesso interessato;
- tutte le informazioni per agevolare l'esercizio dei diritti ai sensi degli articoli da 15 a 22 GDPR;
- ogni comunicazione relativa ad eventuali violazione dei dati personali (data breach) ai sensi dell'art. 34 del RGPD.

Gli interventi necessari per l'attuazione delle misure sono decise dal "Titolare" e considerati nell'ambito della programmazione operativa (D.U.P.), di Bilancio e di Peg, 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. Nel caso in cui un tipo di trattamento, specie se prevede in particolare 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 (da inserire nel "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 11 del presente Regolamento.
6. Il "Titolare", nella persona del Sindaco *pro tempore*, inoltre, provvede a:
   a. designare, con proprio decreto di nomina, ai sensi dell'art. 4 del presente Regolamento, quali "Autorizzati al trattamento" le figure apicali dei Dirigenti/Responsabili di Posizione Organizzativa in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza, nonché eventuali "Sub-autorizzati al trattamento" ai sensi dell'art. 5 del presente Regolamento;
   b. stipulare, in proprio o per il tramite dei soggetti Autorizzati al trattamento, convenzioni, contratti, incarichi professionali o altri strumenti giuridici consentiti dalla legge, con cui i soggetti pubblici o privati sono designati "Responsabili del trattamento esterno", essendo gli stessi deposti al trattamento dei dati personali degli interessati, raccolti in banche dati gestite esternamente al Comune per la realizzazione di attività connesse alle attività istituzionali;
   c. predisporre l'elenco dei soggetti Autorizzati e dei Sub-Autorizzati in forza degli artt. 4 e 5 del presente Regolamento, quali responsabili del trattamento di cui il "Titolare" può avvalersi;

7. Qualora due o più titolari del trattamento determinano congiuntamente, mediante accordo scritto pubblicato nella sezione "Amministrazione Trasparente" del sito istituzionale di questo Ente, le finalità ed i mezzi del trattamento, si realizza la contitolarità del trattamento di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi derivanti dal RGPD, con particolare riferimento all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD (informativa), fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
8. Il "Titolare" 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" e dei Responsabili del trattamento.

Art.3
Ambito applicativo e Finalità del trattamento

Il "Titolare", anche per il tramite dei soggetti Autorizzati e Sub-autorizzati ai sensi degli artt. 4 e 5 del presente Regolamento, raccoglie i dati personali per finalità determinate, esplicite e legittime. I trattamenti dei dati personali operati dal "Titolare" sono compiuti per le seguenti finalità:

a. l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il "Titolare" del trattamento. Rientrano in questo ambito, tra gli altri, i trattamenti compiuti per:
   - 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;
   - la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
   - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune di Cassino in base alla vigente legislazione. 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 di Cassino. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
c. l'esecuzione di un contratto con soggetti interessati;
d. il perseguimento di un legittimo interesse del "Titolare";
e. per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art.4
Autorizzati al trattamento interni all'Ente
(*art. 4, n. 10, del RGPD)*

1. I Dirigenti/Responsabili di Posizione Organizzativa, nell'articolazione organizzativa di rispettiva competenza, sono nominati dal "Titolare" del trattamento, con decreto sindacale contenente le necessarie istruzioni operative, quali "Autorizzati al Trattamento di dati personali con funzioni di responsabilità" di tutti gli archivi cartacei e/o digitali, nonché le banche dati del Comune di Cassino.
2. L'autorizzato al trattamento deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, individuato per iscritto e operare sotto la diretta autorità del "Titolare", attuandone le istruzioni.
3. Possono essere designati quali Autorizzati al Trattamento solo ed esclusivamente le persone fisiche e non anche le entità personificate.
4. Gli Autorizzati sono designati mediante provvedimento di incarico – nella forma di decreto – del Sindaco, nel quale sono tassativamente disciplinati:
   - la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
   - il tipo di dati personali oggetto di trattamento e le categorie di interessati;
5. Il trattamento – da parte dell'autorizzato pubblico dipendente in ruolo presso questo Ente – di dati personali connessi all'espletamento dei compiti istituzionali dell'amministrazione, deve svolgersi sotto la diretta sorveglianza e secondo le istruzioni del Sindaco *pro tempore*, che conserva la qualità di "Titolare del trattamento", non deve comportare decisioni di fondo sulle finalità e sulle modalità di utilizzazione dei dati, ma limitati margini di autonomia in ordine al concreto svolgimento del servizio ed a scelte tecnico-operative dettagliatamente specificate nell'atto formale di designazione.
6. In assenza di una formale designazione come autorizzati al trattamento, i Dirigenti/Responsabili di Posizione Organizzativa che, per lo svolgimento dei propri compiti, vengono a conoscenza di dati personali, devono essere considerati come soggetti terzi rispetto all'Amministrazione, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento.
7. Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il "Titolare" e ciascun Autorizzato designato.
8. Il designato "Autorizzato al Trattamento di dati personali con funzioni di responsabilità" è sottoposto ad obbligo legale di riservatezza.

Art.5

Sub-autorizzati al trattamento interni all'Ente

1. Uno o più dipendenti della struttura organizzativa dell'Ente possono essere nominati "Sub-autorizzati al trattamento" con decreto sindacale o con determina del Dirigente dell'Area di rispettiva competenza ove nominato "Autorizzato al Trattamento di dati personali" e delegato con decreto sindacale del "Titolare" del trattamento, al fine di consentire l'esecuzione materiale di specifiche attività di trattamento per conto del "Titolare" (elabora o utilizza materialmente i dati personali), agendo sotto la sua diretta responsabilità.
2. In assenza di una formale designazione come Sub-autorizzati al trattamento, i dipendenti di questa Pubblica Amministrazione che, per lo svolgimento dei propri compiti, vengono a conoscenza di dati personali, devono essere considerati come soggetti terzi rispetto all'Amministrazione stessa, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento.
3. Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il "Titolare" e ciascun sub-autorizzato designato.
4. Il designato "Sub-autorizzato al Trattamento di dati personali con funzioni di responsabilità" è sottoposto ad obbligo legale di riservatezza.

Art. 6
Responsabile e Sub-responsabili del Trattamento esterno

1. Il "Titolare" può avvalersi, per il trattamento di dati, anche sensibili, di uno o più soggetti pubblici o privati, nominandoli "Responsabili del trattamento esterni", mediante la stipula di apposito contratto in forma scritta (o altro atto giuridico conforme alle norme vigenti) che specifichi la materia disciplinata, la natura, la finalità perseguita, la tipologia dei dati, la categoria degli interessati, la durata del trattamento, gli obblighi, i diritti del "Titolare" del trattamento e le modalità di trattamento.
2. Gli atti che disciplinano il rapporto tra il "Titolare" ed il Responsabile del trattamento esterno devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD e possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione Europea.
3. È consentita la nomina di Sub-responsabili del trattamento esterno da parte di ciascun Responsabile del trattamento esterno per specifiche attività materiali di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il "Titolare" ed il Responsabile del trattamento primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile, attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

4. Il Responsabile esterno risponde, anche dinanzi al "Titolare", dell'operato del sub-responsabile esterno anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile.
5. Il Responsabile del trattamento esterno garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia nominato sub-responsabile del trattamento esterno, ossia persona autorizzata al trattamento esterno, con apposito atto formale in forma scritta e sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
6. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla RGPD e a tutti i compiti affidatigli dal "Titolare", analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
    - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del "Titolare" e a cooperare con l'autorità di controllo mettendo a disposizione tali registri per monitorare detti trattamenti;
    - all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti di cui all'art. 32 RGPD;
    - alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo in qualità di sub-responsabili;
    - ad assistere il "Titolare" nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
    - ad informare il "Titolare", senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il "Titolare" stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati;
    - ad individuare con atto formale i sub-incaricati quali persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del Responsabile del Trattamento esterno.

Art. 7
Responsabile della protezione dati

1. La designazione di un Responsabile della protezione dati (di seguito indicato anche "RPD") è obbligatoria ogni qualvolta il trattamento dei dati personali è effettuato da una autorità pubblica o da un organismo pubblico.

Il Comune di Cassino è obbligato a designare, mediante provvedimento amministrativo, il Responsabile per la Protezione dei Dati nelle seguenti modalità:

a. **RPD interno**

   Il RPD può essere scelto fra i dipendenti dell'Ente di qualifica non inferiore alla cat. D, purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il "Titolare" e/o i soggetti Autorizzati ai sensi dell'art. 4 del presente Regolamento provvedono affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

b. **RPD esterno**

   Il RPD, persona fisica, è selezionato fra soggetti che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili. I compiti attribuiti al RPD sono indicati in apposito contratto di servizi. Il RPD è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al "Titolare" ed al Responsabile del trattamento.

2. Il RPD è incaricato dei seguenti compiti:
   a. informare e fornire consulenza al "Titolare" ed ai soggetti Autorizzati ai sensi dell'artt. 4 del presente Regolamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al "Titolare" ed ai soggetti Autorizzati al trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
   b. sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati personali, fermo restando le responsabilità del "Titolare" e dei soggetti Autorizzati ai sensi dell'artt. 4 del presente Regolamento;
   c. raccogliere informazioni per individuare i trattamenti svolti, analizzare e verificare i trattamenti in termini di loro conformità alla legge, svolgere attività di informazione, consulenza ed indirizzo nei confronti del "Titolare" e dai soggetti Autorizzati ai sensi dell'artt. 4 del presente Regolamento;

d. sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal "Titolare" e dai soggetti Autorizzati ai sensi dell'artt. 4 del presente Regolamento;
e. fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA – valutazione di impatto di trattamento – in inglese: Data Protection Impact Assessment) e sorvegliarne attualità e rispondenza. Il "Titolare", in particolare, si consulta con il RPD in merito a:
   - quale metodologia adottare nel condurre una DPIA;
   - se introdurre o meno uno specifico trattamento all'interno del DPIA;
   - quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
   - se la DPIA sia stata attuata correttamente o meno e se le conclusioni raggiunte (ossia procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi al RGPD;
f. cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto tra questa P.A. e 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;
g. supervisiona circa la regolare tenuta dei registri di cui ai successivi artt. 7 e 8 del presente Regolamento;
h. gli ulteriori compiti e funzioni eventualmente previsti nell'atto di nomina o successivamente comunicati dal "Titolare" o da uno dei soggetti Autorizzati ai sensi dell'artt. 4 del presente Regolamento (in forma scritta a mezzo PEC) ed accettati dal RPD. In tali casi, il "Titolare" o l'Autorizzato al Trattamento devono assicurarsi che tali ulteriori compiti e funzioni non diano adito a conflitto di interessi che possano minare gli obblighi di indipendenza del RPD.

3. Il "Titolare" ed i soggetti Autorizzati assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   a. il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;

b. il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
c. il parere del RPD, eventualmente richiesto sulle decisioni che impattano sulla protezione dei dati, è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta dal "Titolare" determini condotte difformi da quelle raccomandate dal RPD, è necessario che il "Titolare" motivi specificamente tale decisione;
d. il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente lesivo della protezione dei dati.

4. Nello svolgimento dei compiti affidatigli, il RPD 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:
   a. procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
   b. definisce un ordine di priorità nell'attività da svolgere incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al "Titolare" ed al relativo Responsabile del trattamento esterno.
5. La figura di RPD, interno o esterno, è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano incompatibili con tale figura:
   - Il "Titolare" del trattamento;
   - il Responsabile per la prevenzione della corruzione e per la trasparenza;
   - il Responsabile del trattamento esterno;
   - qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
6. Il "Titolare" ed i soggetti Autorizzati ai sensi dell'artt. 4 del presente Regolamento assicurano al RPD:
   - comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
   - accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.
7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti. Il RPD non può essere rimosso o penalizzato dal "Titolare" e dai soggetti Autorizzati ai sensi dell'artt. 4 del presente Regolamento per l'adempimento dei propri compiti.

8. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al "Titolare" – Sindaco *pro tempore* – o ad un suo delegato.
9. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al "Titolare".

Art. 8
Sicurezza del trattamento

1. Il Comune di Cassino, in qualità di "Titolare" del trattamento, nella persona del Sindaco *pro tempore*, e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza idoneo a fronteggiare adeguatamente il 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.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: 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 l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. A tale scopo, per ciascuna Area dell'Ente, vengono effettuate valutazioni dei rischi associati ai vari trattamenti, mediante DPIA ed i Registri di cui ai successivi artt. 8 e 9 del presente Regolamento.
3. A titolo esemplificativo e non esaustivo, costituiscono misure tecniche ed organizzative che possono essere adottate da ciascun Responsabile del trattamento nell'espletamento del proprio servizio:
   - 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.

4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali può essere dimostrata attraverso l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
5. Il "Titolare" e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque sia stato incaricato, con atto formale, ad effettuare accessi in banche dati e trattamenti di dati per conto del "Titolare" e/o del Responsabile del trattamento.
6. I dati di contatto del "Titolare" e dei soggetti Autorizzati ai sensi dell'artt. 4 del presente Regolamento e del Responsabile della Protezione dati sono pubblicati sul sito istituzionale dell'Ente, sezione Amministrazione trasparente, oltre che nella sezione "privacy".
7. 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 (ex artt. 20 e 22, D.Lgs. n. 193/2006).

Art. 9
Registro delle attività di trattamento

1. Il Registro delle attività di trattamento è il documento contenente le principali informazioni (specificate dall'art. 30 RGPD) relative alle operazioni di trattamento dei dati relativi alle singole aree di riferimento (come da organigramma) nel rispetto delle deleghe effettuate dal "Titolare". Si tratta, dunque, di una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati ed ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.
2. Il Registro delle attività di trattamento reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto del "Titolare", dei soggetti Autorizzati ai sensi del precedente art. 4 del presente Regolamento (Dirigenti/Titolari di Posizione Organizzativa), del RPD ed eventualmente del Contitolare del trattamento, nonché dei Responsabili esterni;
   b) le finalità del trattamento e l'elenco delle attività;
   c) una descrizione delle categorie di interessati e delle categorie di dati personali;
   d) le categorie di trattamenti effettuati da ciascun Responsabile, quali raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
   e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

f) l'eventuale trasferimento di dati personali verso un Paese terzo od una organizzazione internazionale;
g) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
h) ove possibile, il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

3. Il Registro è tenuto dal "Titolare" ovvero da un soggetto Autorizzato ai sensi del precedente art. 4 (Dirigente/Responsabili di Posizione Organizzativa) per la parte relativa alla propria area di competenza, presso gli uffici della struttura organizzativa dell'Ente, in forma telematica o cartacea, secondo lo schema allegato "A" al presente Regolamento.
4. Il "Titolare" del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo "Titolare".
5. Ciascun Responsabile del trattamento esterno ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto alla tenuta di tale Registro ogni elemento necessario alla regolare tenuta ed all'aggiornamento dello stesso.

Art. 10
Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il "Titolare" o il soggetto da questi Autorizzato della competente Area, prima di effettuare il trattamento, deve attuare una valutazione d'impatto sulla protezione dei dati (c.d. Data Protection Impact Assessment, di seguito anche "DPIA") ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA, trattandosi di una valutazione preliminare relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati, è una procedura che permette di realizzare e dimostrare la conformità del trattamento di cui trattasi alle norme del RGPD.
2. Ai fini della decisione di effettuare o meno la DPIA in relazione ad uno specifico trattamento, si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione ove redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.
3. La DPIA è obbligatoriamente effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato sono i seguenti:

a. trattamenti di valutazione sistematica, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c. monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d. trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
e. trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f. combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g. dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il "Titolare" del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i. tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

4. Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una valutazione d'impatto sulla protezione dei dati ed inserire il trattamento nel relativo Documento, salvo che il "Titolare" ritenga, con atto motivato scritto, che non possa presentare un rischio elevato; del pari, il "Titolare" può, con atto motivato scritto, ritenere che per un trattamento che soddisfi solo uno dei criteri di cui sopra occorra comunque la conduzione di una valutazione d'impatto sulla protezione dei dati.
5. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
- 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 valutazione d'impatto sulla protezione dei dati. In questo caso, si possono utilizzare i risultati della DPIA già svolta per l'analogo trattamento;
- 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;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una valutazione d'impatto sulla protezione dei dati all'atto della definizione della base giuridica suddetta

Non è necessario condurre una valutazione d'impatto sulla protezione dei dati per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente.

Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

6. La valutazione d'impatto sulla protezione dei dati è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
    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. valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

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 RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

7. Il "Titolare" garantisce l'effettuazione della valutazione d'impatto sulla protezione dei dati ed è responsabile della stessa. Il "Titolare" può affidare la conduzione materiale della valutazione ad un altro soggetto, interno o esterno al Comune. Il "Titolare" può consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal "Titolare" devono essere documentate nell'ambito del relativo Documento.
8. Il RPD monitora lo svolgimento della DPIA. Il Responsabile del trattamento esterno deve assistere il "Titolare" nella conduzione della DPIA fornendo tempestivamente, entro 5 giorni dalla richiesta, ogni informazione necessaria.
9. Il Responsabile della sicurezza dei sistemi informativi dell'Ente, se nominato, e/o l'Ufficio competente per detti sistemi, forniscono supporto al "Titolare" per lo svolgimento della DPIA.
10. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Il Responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
11. Il "Titolare" può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
12. Il "Titolare" deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il

"Titolare" consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

13. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 11
Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o illecitamente 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 il soggetto Delegato ai sensi dell'art. 4 del presente Regolamento, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy.

   La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento esterno (quando di pertinenza) è obbligato ad informare il "Titolare" e il RPD, entro e non oltre 72 ore e comunque senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
   - danni fisici, materiali o immateriali alle persone fisiche;
   - perdita del controllo dei dati personali;
   - limitazione dei diritti, discriminazione;
   - furto o usurpazione d'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. Se il “Titolare” ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.

   I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

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

5. La notifica deve avere il contenuto minimo previsto dall’art. 33 RGPD, ed anche la comunicazione all’interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33 RGPD.
6. Il “Titolare” deve, in ogni caso, opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle Autorità di controllo, in quanto non rientranti nelle ipotesi di cui sopra, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio.

Art. 12
Rinvio

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

GLOSSARIO REGOLAMENTO

Ai fini della proposta di Regolamento comunale, si intende per:

◊ **Titolare del trattamento:**

Autorità pubblica (Sindaco *p.t.*) che, singolarmente o insieme ad altri, determina finalità e mezzi del trattamento di dati personali.

◊ **Responsabile del trattamento esterno:**

Soggetto pubblico o privato che tratta dati personali per conto del Titolare del trattamento in ragione di un contratto di fornitura e/o di servizi.

◊ **Sub-Responsabile del trattamento esterno:**

Incaricato dal Responsabile del trattamento esterno con atto formale, per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento (elabora o utilizza materialmente i dati personali).

◊ **Autorizzato al trattamento con funzioni di responsabilità:**

Dirigente/Responsabile di Posizione Organizzativa che tratta dati personali per conto del Titolare del trattamento.

◊ **Sub- autorizzato al trattamento:**

Dipendente della struttura organizzativa dell'Ente incaricato dal Titolare del trattamento con decreto sindacale ovvero da soggetto Autorizzato al trattamento con determina dirigenziale, per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento (elabora o utilizza materialmente i dati personali).

◊ **Responsabile per la protezione dati – RPD:**

Dipendente della struttura organizzativa dell'Ente, professionista privato o persona fisica di impresa esterna incaricati dal Titolare o dal Responsabile del trattamento esterno.

◊ **Registri delle attività di trattamento**:

Elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento esterno secondo le rispettive competenze.

◊ **Data Protection Impact Assessment – c.d. "DPIA"**:

Valutazione d'impatto sulla protezione dei dati, ossia procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

◊ **Garante Privacy:**

Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996, n. 675, quale Autorità amministrativa pubblica di controllo indipendente.

GLOSSARIO REGISTRI

Ai fini delle proposte dei registri, si intende per:

◊ **Categorie di trattamento:**

Raccolta; registrazione; organizzazione; strutturazione; conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto od interconnessione;

limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.

◊ **Categorie di dati personali:**

Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale.

Dati inerenti lo stile di vita: situazione economica, finanziaria, patrimoniale, fiscale.

Dati di connessione: indirizzo IP, login, altro.

Dati di localizzazione: ubicazione, GPS, GSM, altro.

Dati sensibili: origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici intesi ad indentificare in modo univoco una persona fisica, dati relativi alla salute, relativi alla vita sessuale o all'orientamento sessuale della persona, relativi a condanne penali.

◊ **Finalità del trattamento:**

Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico; la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica; l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune.

Adempimento di un obbligo legale al quale è soggetto il Comune.

Esecuzione di un contratto con i soggetti interessati. Altre specifiche e diverse finalità.

◊ **Misure tecniche ed organizzative:**

Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi.

Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.

Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori

dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico - adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.

Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

◊ **Categorie di interessati:**

Cittadini residenti; minori di anni 16; elettori; contribuenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; altro.

◊ **Categorie di destinatari:**

Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.