Allegato alla DCC n. 21/2018 del 25/07/2018

COMUNE DI PARODI LIGURE

REGOLAMENTO PER LA PROTE-ZIONE DEI DATI PERSONALI

indice

ARTICOLO 1. OGGETTO

1. Il presente Regolamento ha per oggetto la disciplina di misure organizzative e di regole di dettaglio per l'attuazione del Regolamento europeo General Data Protection Regulation del 27 aprile 2016 n. 679 [d'ora innanzi: GDPR] relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati.
2. Il presente regolamento è adottato nell'ambito della potestà regolamentare in capo al Comune, prevista dall'articolo 7 del D.Lgs. 18 agosto 2000, n. 267, e s.m.i (testo unico delle leggi sull'ordinamento degli enti locali) [d'ora innanzi: D.Lgs. 267/2000].
3. Ai fini del presente regolamento, ferme le definizioni dell'articolo 4 del GDPR, valgono, ove non diversamente stabilito, le seguenti definizioni:
   a) per "Comune" il Comune di Parodi Ligure;
   b) per "titolare del trattamento", il Comune, autorità pubblica che, singolarmente o insieme ad altro soggetto avente titolo per legge o per rapporto giuridicamente rilevante, determina le finalità e i mezzi del trattamento di dati personali di cui viene in possesso;
   c) per "responsabile del trattamento", qualunque soggetto, interno o esterno al Comune, purché collegato al Comune da rapporto giuridicamente rilevante e conforme alla normativa, incaricato della relativa funzione;

ARTICOLO 2. TITOLARE DEL TRATTAMENTO

1. Il Comune, rappresentato ai fini previsti dal GDPR dal Sindaco pro tempore, o suo sostituto legale, oppure dalla Giunta Comunale è il titolare del trattamento dei dati personali raccolti, compresi quelli raccolti in banche dati, informatizzate o cartacee.
2. Il titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'articolo 5 GDPR, e, in particolare, ai sensi dell'articolo 5 comma 1 GDPR:
   a) della liceità, della correttezza e della trasparenza;
   b) della limitazione della finalità, ivi compresa la finalità di archiviazione nel pubblico interesse;
   c) della minimizzazione dei dati;
   d) della esattezza;
   e) della limitazione della conservazione, ivi compresa la finalità di archiviazione nel pubblico interesse;
   f) della integrità e della riservatezza.
3. In attuazione dell'articolo 24 comma 1 GDPR Il titolare mette in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR.
4. Ai fini del comma 4 del presente articolo, sulla base delle previsioni del Documento Unico di Programmazione (DUP), è stanziato apposito budget in sede di bilancio di previsione e previsto idoneo capitolo in sede di Piano esecutivo di Gestione (PEG).
5. Gli interventi, ai sensi dell'articolo 24 comma 1 GDPR, sono programmati sulla base di apposita analisi preventiva della situazione in essere, e tenuto conto:

a) dei costi di attuazione

b) della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento;

c) dei rischi derivanti dal trattamento, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

6. Ai fini della valutazione dell'adeguatezza di cui al comma 4 del presente articolo, sulla base dei parametri di cui all'articolo 24 comma 1 GDPR, di cui al comma 6 del presente articolo, il titolare si avvale, nel limite del budget di cui di cui al comma 4 del presente articolo, del supporto di operatore economico qualificato.
7. In attuazione dell'articolo 25 comma 1 GDPR il titolare cura che le misure siano definite fin dalla fase di progettazione e siano messe in atto per applicare in modo efficace i principi di protezione dei dati.
8. Il titolare cura che le misure siano messe in atto, altresì, per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli dal 15 al 22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio, in particolare adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.
9. 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 (di seguito indicata con "DPIA") ai sensi dell'articolo 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dall'articolo 9 del presente regolamento.
10. Ai sensi dell'articolo 24 comma 3 GDPR l'azione del Comune è informata all'adesione agli eventuali codici di condotta elaborate dai soggetti all'uopo titolati di cui all'articolo 40 GDPR, nonché, nei limiti delle risorse disponibili, all'adozione di meccanismi di certificazione di cui all'articolo 42 GDPR.
11. Il Titolare provvede a:
    a) designare i Responsabili del trattamento, anche avvalendosi di soggetti pubblici o privati, ai sensi dell'articolo 3 del presente regolamento;
    b) nominare il Responsabile della protezione dei dati;
    c) predisporre l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.
12. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'articolo 26 comma 1 GDPR.
13. L'accordo di cui di cui al comma 13 del presente articolo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le

rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR.

14. l'accordo di cui al comma 13 del presente articolo può individuare un punto di contatto comune per gli interessati.

ARTICOLO 3. FINALITÀ DEL TRATTAMENTO

1. I trattamenti sono compiuti dal Comune per le seguenti finalità:
- **a)** l'esecuzione di un compito di interesse pubblico, o connesso all'esercizio di pubblici poteri;
- **b)** l'adempimento di un obbligo legale al quale è soggetto il Comune;
- **c)** l'esecuzione di un contratto con soggetti interessati;
- **d)** finalità diverse da quelle di cui alle precedenti lettere a), b), c).

2. Rientrano nell'ambito della lettera a) del comma 1 del presente articolo, i trattamenti compiuti ai fini:
- **a)** dell'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, in particolare nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
- **b)** della gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
- **c)** dell'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

3. Ai fini di cui alla lettera b) del comma 1 del presente articolo, la finalità del trattamento è stabilita dalla fonte normativa che lo disciplina.

4. Ai fini di cui alla lettera d) del comma 1 del presente articolo, il trattamento è consentito a condizione che l'interessato esprima il consenso al trattamento.

ARTICOLO 4. RESPONSABILE DEL TRATTAMENTO

1. In modalità ordinaria, ciascun responsabile di servizio, incaricato di posizione organizzativa, è nominato Responsabile del trattamento della integralità delle banche dati personali esistenti nell'articolazione organizzativa di propria competenza.

2. In casi particolari, con particolare riferimento alle attività di natura non permanente, quali, ad esempio, le procedure di selezione del contraente, le procedure di selezione del personale, i concorsi a premi, le mostre, le manifestazioni, i servizi temporanei, possono essere nominati quali responsabili del trattamento, limitatamente ai dati personali, anche sensibili, dei relativi procedimenti, dipendenti non incaricati di posizione organizzativa aventi la professionalità del funzionario, corrispondente alle categorie professionali C o D, di cui alle declaratorie allegate al C.C.N.L. del comparto Regioni Autonomie Locali stipulato in data 31.03.1999.

3. In caso di esternalizzazione parziale di servizi e di attività rientranti nelle finalità istituzionali del Comune, svolte, per conto del Comune stesso, sia da operatori economici privati, sia da enti pubblici, sulla base di convenzioni, di contratti, di incarichi professionali o di altri istituti giuridici comunque consentiti dalla legge, possono essere nominati quali responsabili del

trattamento, in relazione ai dati personali, anche sensibili, coinvolti nelle relative procedure e attività, comprese le banche dati, soggetti estranei al Comune, incardinati con sufficiente grado di stabilità nella struttura organizzativa del soggetto incaricato.

4. Al di fuori delle ipotesi di cui di cui al comma 3 del presente articolo il titolare può comunque avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 5, sulla base di convenzioni, di contratti, di incarichi professionali o di altri istituti giuridici comunque consentiti dalla legge.

5. Nei casi di cui ai commi 3 e 4 del presente articolo il Responsabile del trattamento deve essere comunque in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'articolo 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

6. I responsabili del trattamento dipendenti del Comune sono designati, di norma, mediante decreto di incarico del Sindaco, oppure, nei casi di cui al comma 2 del presente articolo, del segretario comunale.

7. I responsabili del trattamento non dipendenti del comune, individuati ai sensi dei commi 3 e 4 del presente articolo, sono designati mediante l'apposito contratto, o convenzione, o altra forma prevista dalla legge, regolante l'incarico di esternalizzazione, avente i contenuti di cui al comma 9 del presente articolo.

8. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'articolo 28 comma 3 GDPR; possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea, e, in ogni caso, indicare:

- **a)** la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- **b)** la modalità di trattamento;
- **c)** il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- **d)** gli obblighi ed i diritti del Titolare del trattamento.

9. Il Responsabile del trattamento può, a propria volta, nominare sub responsabili del trattamento per specifiche attività di trattamento, fermo il rispetto degli stessi obblighi intercorrenti fra titolare e responsabile, con le seguenti ulteriori prescrizioni:

- **a)** 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, individuanti specificatamente l'ambito del trattamento consentito;
- **b)** il responsabile del trattamento risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salva dimostrazione della assoluta non imputabilità a sé medesimo dell'evento dannoso e di avere vigilato adeguatamente sull'operato del sub responsabile;
- **c)** il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

ARTICOLO 4BIS. COMPITI DEL RESPONSABILE DEL TRATTAMENTO

1. Il Responsabile del trattamento provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge ed a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- **a)** alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- **b)** all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- **c)** alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- **d)** alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;
- **e)** 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;
- **f)** 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.

ARTICOLO 5 RESPONSABILE DELLA PROTEZIONE DATI

1. Il Responsabile della protezione dei dati è individuato nella figura unica, di professionista scelto tramite procedura di selezione conforme alla normativa vigente in materia di contratti pubblici.

2. Il Responsabile della protezione dei dati è incaricato dei seguenti compiti:

- **a)** informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, e dalle altre normative relative alla protezione dei dati;
- **b)** sorvegliare l'osservanza del GDPR, e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento;
- **c)** sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;
- **d)** fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- **e)** cooperare con il Garante per la protezione dei dati personali e svolgere per conto del medesimo il ruolo di punto di contatto relativamente alle questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione;
- **f)** la tenuta dei registri di cui ai successivi articoli 7 e 8;

g) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi.

3. Ai fini di cui alla lettera a) del comma 2 del presente articolo, il Responsabile della protezione dei dati può indicare al Titolare e/o al Responsabile del 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;

4. Fanno parte dei compiti di cui alla lettera b) del comma 2 del presente articolo:

a) la raccolta di informazioni per individuare i trattamenti svolti;

b) l'analisi e la verifica dei trattamenti in termini di loro conformità;

c) l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento.

5. In merito alla valutazione di impatto sulla protezione dei dati di cui alla lettera d) del comma 2 del presente articolo, il Titolare si consulta con il Responsabile della protezione dei dati in merito a:

a) alla decisione se condurre o meno la valutazione;

b) quale metodologia adottare nel condurre la valutazione;

c) se condurre la la valutazione con le risorse interne ovvero ricorrendo alla esternalizzazione;

d) quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;

e) se la valutazione sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare siano conformi al GDPR.

6. Ai fini di cui alla lettera e) del comma 2 del presente articolo, il nominativo del RPD è comunicato dal Titolare, o dal Responsabile del trattamento al Garante per la protezione dei dati personali.

7. L'assenza di conflitti di interessi di cui alla lettera g) del comma 2 del presente articolo, è strettamente connessa agli obblighi di indipendenza del Responsabile della protezione dei dati.

8. Il Titolare ed il Responsabile del trattamento assicurano che il Responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, e, a tali fini, il Responsabile della protezione dei dati:

a) è invitato a partecipare alle riunioni di coordinamento degli organi del Comune, compresi i Responsabili di servizio, aventi ad oggetto questioni inerenti la protezione dei dati personali;

b) deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, ai fini di essere in grado di rendere idonea consulenza, scritta od orale;

c) in merito alle decisioni che impattano sulla protezione dei dati esprime parere obbligatorio ma non vincolante, e, pertanto, nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal Responsabile della protezione dei dati, tale decisione deve essere motivata;

d) deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o altro incidente.

9. Nello svolgimento dei compiti affidatigli il Responsabile della protezione dei dati deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo, e, a tali fini, Responsabile della protezione dei dati:

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, ovvero un piano annuale di attività, incentrati sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

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

11. La figura di Responsabile della protezione dei dati è incompatibile con chi determina le finalità od i mezzi del trattamento, e, in particolare, risultano incompatibili con la figura del Responsabile della protezione dei dati:

a) il Responsabile per la prevenzione della corruzione e per la trasparenza;

b) il Responsabile del trattamento;

c) qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

12. Il Titolare ed il Responsabile del trattamento forniscono al Responsabile della protezione dei dati le risorse necessarie ai fini di assolvere ai compiti attribuiti ed ai fini di accedere ai dati personali ed ai trattamenti, e, in particolare, è assicurato al RPD:

a) il supporto attivo per lo svolgimento dei compiti da parte della Giunta Comunale, del segretario, dei responsabili di servizio, in coerenza con l'attuazione delle attività necessarie alla protezione dati nell'ambito del DUP e del PEG;

b) il tempo necessario per consentire l'espletamento dei compiti affidati al RPD;

c) -il supporto adeguato in termini di risorse finanziarie, di infrastrutture, quali attrezzature e strumentazione e, ove necessiti, di personale;

d) la comunicazione ufficiale della nomina alla integralità del personale, ai fini di rendere noti la presenza e le funzioni relative;

e) l'accesso garantito ai settori funzionali del Comune ai fini di supporto, informazioni e input essenziali.

13. Il Responsabile della protezione dei dati, inoltre:

a) opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti, e, in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da fornire a specifiche problematiche attinenti la normativa in materia di protezione dei dati personali;

b) non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti;

c) ferma restando l'indipendenza nello svolgimento di detti compiti, riferisce direttamente al Titolare, in persona del Sindaco o di suo delegato, o del segretario comunale, o, in subordine, al Responsabile del trattamento.

14. Nel caso in cui siano rilevate dal Responsabile della protezione dei dati, o sottoposte alla sua attenzione, decisioni incompatibili con il GDPR, oppure con le indicazioni fornite dallo stesso Responsabile della protezione dei dati, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

ARTICOLO 6. SICUREZZA DEL TRATTAMENTO

1. Il Comune, in persona degli organi di governo, del segretario, dei Responsabili del trattamento, mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché 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:

a) la pseudonimizzazione, la minimizzazione, la cifratura dei dati personali;

b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

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

3. Costituiscono misure tecniche ed organizzative, che devono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:

a) misure informatiche: sistemi di autenticazione, sistemi di autorizzazione, sistemi di protezione, quali antivirus, firewall, antintrusione;

b) misure fisiche: misure antincendio, sistemi di rilevazione di intrusione, sistemi di sorveglianza; sistemi di videosorveglianza e di registrazione degli accessi, porte, armadi, contenitori dotati di serrature e ignifughi;

c) misure di backup: sistemi di copiatura e conservazione di archivi elettronici;

d) 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 è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. Il Comune, in persona degli organi di governo, del segretario, dei Responsabili del trattamento, si obbliga ad impartire adeguate istruzioni sul rispetto delle misure di cui al presente articolo a chiunque agisca per conto del Comune ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito

istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione “privacy” eventualmente già presente.

ARTICOLO 7. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca le seguenti informazioni minime:
- **a)** il nome ed i dati di contatto del Comune, del Sindaco, del suo delegato ai sensi dell’articolo 2 del presente regolamento, ove presente, del contitolare del trattamento, del Responsabile della protezione dei dati;
- **b)** le finalità del trattamento;
- **c)** la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- **d)** le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- **e)** l’eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- **f)** ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- **g)** il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, ai sensi dell’articolo 6.

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi dell’articolo 2 del presente regolamento, presso gli uffici della struttura organizzativa del Comune in forma telematica, oppure cartacea, secondo lo schema allegato A al presente Regolamento.

3. Il Titolare del trattamento può affidare al Responsabile della protezione dei dati il compito di tenuta del Registro, sotto la responsabilità del medesimo Titolare.

ARTICOLO 8. REGISTRO DELLE CATEGORIE DI ATTIVITÀ TRATTATE

1. Il Registro delle categorie di attività trattate da ciascun Responsabile del trattamento, reca le seguenti informazioni:
- **a)** il nome ed i dati di contatto del Responsabile del trattamento e del Responsabile della protezione dei dati;
- **b)** le categorie di trattamenti effettuati da ciascun Responsabile: 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;
- **c)** l’eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- **d)** il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, ai sensi dell’articolo 5 del presente regolamento.

2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica oppure cartacea, secondo lo schema allegato B al presente regolamento.

3. Il Responsabile del trattamento Il Titolare del trattamento può affidare al Responsabile della protezione dei dati il compito di tenuta del Registro, sotto la responsabilità del medesimo Responsabile del trattamento.

ARTICOLO 9. VALUTAZIONI D'IMPATTO SULLA PROTEZIONE DEI DATI

1. Nel caso in cui un tipo di trattamento, specialmente ove preveda l'uso di nuove tecnologie, presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del trattamento sulla protezione dei dati ai sensi dell'articolo 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

2. La valutazione dell'impatto del trattamento sulla protezione dei dati è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento.

3. Ai fini della decisione di effettuare o meno la valutazione si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante per la protezione dei dati personali ai sensi dell'articolo 35 commi 4,5, 6 GDPR.

4. La valutazione è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche.

5. Fermo restando quanto indicato dall'articolo 35 comma 3 GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

- **a)** trattamenti valutativi o di scoring, 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'articolo 9 GDPR;
- **e)** trattamenti di dati su larga scala, tenendo conto: del numero di 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.

6. Nel caso in cui un trattamento soddisfi almeno due dei criteri indicati dal comma 5 del presente articolo occorre, in via generale, condurre una valutazione dell'impatto del trattamento sulla protezione dei dati, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato.

7. Il Titolare può altresì motivatamente ritenere che per un trattamento che soddisfa soltanto dei criteri indicati al comma 5 del presente articolo occorra comunque la conduzione di una valutazione dell'impatto del trattamento sulla protezione dei dati.

8. Il Titolare garantisce l'effettuazione della valutazione dell'impatto del trattamento sulla protezione dei dati ed è responsabile della stessa.

9. Il Titolare può affidare la conduzione materiale della valutazione ad un altro soggetto, interno o esterno al Comune.

10. Il Titolare deve consultarsi con il Responsabile della protezione dei dati anche per assumere la decisione di effettuare o meno la valutazione.

11. La consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della valutazione.

12. Il Responsabile della protezione dei dati monitora lo svolgimento della valutazione.

13. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della valutazione, fornendo ogni informazione necessaria.

14. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della valutazione.

15. 5. Il Responsabile della protezione dei dati può proporre lo svolgimento di una valutazione dell'impatto del trattamento sulla protezione dei dati 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.

16. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una valutazione dell'impatto del trattamento sulla protezione dei dati in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

17. La valutazione dell'impatto del trattamento sulla protezione dei dati non è necessaria nei casi seguenti:

a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'articolo 35 comma 1, GDPR;

b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una valutazione dell'impatto del trattamento sulla protezione dei dati, in questo caso potendosi utilizzare i risultati della valutazione svolta per l'analogo trattamento;

c) se il trattamento è stato sottoposto a verifica da parte del Garante per la protezione dei dati personali prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;

d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una valutazione dell'impatto del trattamento sulla protezione dei dati all'atto della definizione della base giuridica suddetta.

18. Non è necessario condurre una valutazione per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante per la protezione dei dati personali o da un Responsabile della protezione dei dati e che proseguano con le stesse modalità oggetto di tale verifica, tenendo altresì conto della permanenza in vigore, fino a modifica, sostituzione o abrogazione, delle autorizzazioni del Garante per la protezione dei dati personali fondate sulla direttiva 95/46/CE.

19. La valutazione dell'impatto del trattamento 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, altresì indicando: 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;

c) consultazione preventiva del Garante per la protezione dei dati personali;

d) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati, determinando 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;

e) 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 di altri soggetti interessati.

20. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati.

21. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

22. Il Titolare deve consultare il Garante per la protezione dei dati personali prima di procedere al trattamento se le risultanze della valutazione dell'impatto del trattamento sulla protezione dei dati condotta indicano l'esistenza di un rischio residuale elevato.

23. Il Titolare consulta il Garante per la protezione dei dati personali 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.

24. La valutazione dell'impatto del trattamento sulla protezione dei dati 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.

ARTICOLO 10. VIOLAZIONE DEI DATI PERSONALI

1. Per violazione dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.

2. Il Titolare, 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 per la protezione dei dati personali.

3. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.

4. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

5. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, 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).

6. 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, finanziari, relativi alle 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).

7. La notifica deve avere il contenuto minimo previsto dall'articolo 33 GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato articolo 33.

8. 6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio.

9. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante per la protezione dei dati personali al fine di verificare il rispetto delle disposizioni del GDPR.

ARTICOLO 11. DISPOSIZIONE FINALE TRANSITORIA

1. Per quanto non previsto dal presente regolamento si applicano le disposizioni di legge vigenti.

2. 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 ai sensi degli articoli 20 e 22 D.Lgs. 193/2006, e s.m.i.).