Comune di Monte Romano

Provincia di Viterbo

Regolamento per il trattamento e la protezione dei dati personali in attuazione del Regolamento UE 2016/679

(Delibera del Consiglio Comunale n. 02 del 19/03/2019)

SOMMARIO

ALLEGATI:

A) schema di registro attività di trattamento

B) schema di registro categorie attività di trattamento

C) schema di registro unico di trattamento

Art. 1
Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini dell'efficace attuazione da parte del Comune di Monte Romano del Regolamento europeo del 27 aprile 2016 n. 679 (di seguito indicato con "GDPR", General Data Protection Regulation), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati (che ha abrogato la Direttiva 95/46/CE).

2. In particolare, il presente Regolamento disciplina il trattamento dei dati personali contenuti nelle banche dati organizzate, gestite e utilizzate dall'Amministrazione comunale e da soggetti esterni dalla stessa specificamente individuati – incaricati dello svolgimento di determinate attività in nome e per conto del Comune, dunque in qualità di Responsabili del trattamento *ex* art. 28 del GDPR - in relazione allo svolgimento delle proprie attività istituzionali, in applicazione:

- della normativa in materia di diritto di accesso documentale (accesso agli atti amministrativi ai sensi della L. 241/1990; accesso civico e accesso generalizzato ai sensi del D. Lgs. 33/2013, come modificato dal D. Lgs. 97/2016);
- della normativa in materia di trattamento, protezione e libera circolazione dei dati personali, quale risultante dal GDPR e dal D. Lgs. 196/2003, come modificato dal D. Lgs. 101/2018;
- delle norme di legge e regolamentari, nazionali e locali, che disciplinano lo svolgimento delle attività amministrativa e di governo da parte delle amministrazioni comunali.

Art. 2
Definizioni

1. Ai fini del presente Regolamento si intende per:

a) "***trattamento***": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

b) "***dato personale***": qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di

identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

c) "***dati identificativi***": i dati personali che permettono l'identificazione diretta dell'interessato;

d) "***dati particolari***" (di cui all'art. 9 del GDPR): dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché 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 (categoria indicata, nel vigore della precedente normativa, come "dati sensibili").

e) "***dati relativi a condanne penali e reati***"(di cui all'art. 10 del GDPR): dati personali relativi a condanne penali e reati o a connesse misure di sicurezza.

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

g) "***responsabile del trattamento***": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

h) "***incaricati / designati al trattamento***": le persone fisiche, espressamente designate, autorizzate a compiere, mediante l'attribuzione di specifici compiti e funzioni, operazioni di trattamento dal titolare o dal responsabile, sotto la loro autorità;

i) "***interessato***": la persona fisica a cui si riferiscono i dati personali;

j) "***consenso dell'interessato***": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

k) "***dato anonimo***": il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile*;*

l) "***blocco***"*:* la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

m) "***banca dati***": qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

n) "***Garante***": l'autorità italiana preposta al controllo delle modalità di trattamento e di protezione dei dati personali, ai fini della tutela dei diritti degli interessati;

o) "***violazione di dati personali***" (c.d. "*data breach*"): violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.

p) "***profilazione***": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

q) "***pseudonimizzazione***": il trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Art.3
Finalità

1. Il Comune, nell'assolvimento delle proprie finalità istituzionali, nel rispetto dei principi di trasparenza, efficacia ed economicità dell'azione amministrativa, garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il rispetto del diritto alla riservatezza e all'identità personale, nonché delle norme vigenti in materia di gestione e protezione dei dati in parola.
2. Nell'adempimento degli obblighi di comunicazione interna ed esterna e si semplificazione dell'azione amministrativa, il Comune di Monte Romano favorisce la trasmissione di dati e documenti tra le banche dati e gli archivi del Comune, degli enti territoriali, degli enti pubblici, dei gestori e degli incaricati di pubblico servizio operanti nello Stato italiano e/o all'interno dell'Unione Europea.
   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.
3. Ai fini del presente Regolamento, per finalità istituzionali del Comune si intendono le funzioni ad esso attribuite da leggi e regolamenti, dallo Statuto o per effetto di accordi e/o convenzioni e/o contratti.
4. I trattamenti sono effettuati dal Comune per le seguenti finalità:
   a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.
   Rientrano in questo ambito 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 in base alla vigente legislazione*.

   La singola, specifica 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 singola, specifica finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

c) l'esecuzione di un contratto o di misure precontrattuali con soggetti interessati;

d) la necessità di effettuare il trattamento per motivi di interesse pubblico rilevante;

e) finalità di archiviazione nel pubblico interesse, di ricerca storica, di statistica;

f) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art.4
Titolare del trattamento

1. Il Comune di Monte Romano, rappresentato ai fini previsti dal GDPR dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti e/o conservati e/o gestiti attraverso banche dati, cartacee o informatiche (di seguito indicato con "Titolare"). Il Sindaco può delegare le relative funzioni a Responsabile P.O. in possesso di adeguate competenze.
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.
2. 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.
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 del RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), 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.
3. Il Titolare adotta misure appropriate per fornire all'interessato:
   - le informazioni indicate dall'art. 13 del GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
   - le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.
4. 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'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 14.
5. Il Titolare, inoltre, provvede a:

- designare i Responsabili del trattamento (interni) nelle persone dei Dirigenti/Responsabili P.O. e dei Funzionari delle singole strutture (Aree / Servizi) 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;
- nominare il Responsabile della protezione dei dati;
- nominare quali Responsabili del trattamento (esterni) i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

6. 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'art. 26 RGPD. L'accordo 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 artt. 13 e 14 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

7. Il Comune 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 GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 5
Responsabile del trattamento

1. Uno o più Responsabili P.O. dell'Ente sono designati, ai sensi dell'art. 28 del GDPR e dell'art. 2 - *quaterdecies* del Decreto Legislativo 30 giugno 2003 n. 196, come modificato e integrato dal Decreto Legislativo 10 agosto 2018, n. 101, quali Responsabili del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile deve essere 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'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

2. I dipendenti del Comune, Responsabili del trattamento, sono designati di norma mediante decreto di incarico del Sindaco, nel quale sono individuati i compiti e le funzioni affidate a ciascuno di essi, in relazione ai Settori di competenza, con riferimento alle attività di trattamento ad essi demandate come individuate dalle apposite sezioni del Registro delle attività di trattamento del Comune.

3. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge 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;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- alla designazione del Responsabile per la Protezione dei Dati (RPD/DPO), se a ciò demandato dal Titolare;
- 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, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

4. Il Titolare può avvalersi, inoltre, per il trattamento di dati, anche particolari (*ex* "dati sensibili"), di soggetti pubblici o privati esterni che, in qualità di responsabili del trattamento, forniscano le garanzie di cui all'art. 32 del GDPR, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.

5. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono, in particolare, contenere quanto previsto dall'art. 28, p. 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

6. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile 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.

Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

7. 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.

Art.6
Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con “RPD”/ “DPO”) è selezionato all’esterno tramite procedura ad evidenza pubblica, ovvero - a scelta dell’Amministrazione – è individuato tra i dipendenti di ruolo del Comune che risultino in possesso di adeguate competenze quanto alla conoscenza e applicazione della normativa vigente in materia di trattamento e protezione dei dati personali.

Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare e ai Responsabili del trattamento, nonché ai dipendenti che eseguono il trattamento (in qualità di incaricati / designati) 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 e/o ai Responsabili 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;
b) sorvegliare l’osservanza e applicazione delle previsioni del GDPR e delle altre disposizioni normative relative alla protezione dei dati personali, ferma restando la responsabilità del Titolare e dei Responsabili del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l’analisi e la verifica dei trattamenti in termini di loro conformità, l’attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
c) sorvegliare le attribuzioni di compiti e responsabilità all’interno dell’organizzazione, le attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e/o dai Responsabili del trattamento;fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA 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;
d) cooperare con il Garante per la protezione dei dati personali e ricoprire il ruolo di punto di contatto per detta Autorità per questioni connesse al trattamento dei dati personali, tra cui la consultazione preventiva di cui all’art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;
e) coadiuvare il Titolare e i Responsabili (interni) nella tenuta dei registri di cui al successivo art. 13;
f) 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. L’assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

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

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Responsabili P.O. che abbiano per oggetto questioni inerenti il trattamento e la protezione dei dati personali;
- 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;
- il parere del RPD 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, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. 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 - 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.

4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e comunque compatibilmente delle capacità di bilancio dell'Ente.

5. La figura di RPD è incompatibile con chi determina le finalità od 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. Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;
- tempo sufficiente per l'espletamento dei compiti affidati al RPD;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- 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; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Il RPD non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare (il Sindaco o suo delegato, oppure il Segretario comunale nella sua veste di Coordinatore designato per lo svolgimento delle varie attività).

Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare.

Art.7
Incaricati /designati al trattamento

1. Sono incaricati del compimento delle operazioni di trattamento dei dati i soggetti (dipendenti e collaboratori a qualsiasi titolo) che operano nel Comune di Monte Romano sotto l'autorità del Titolare e/o dei Responsabili interni, appositamente designati e/o espressamente autorizzati, in ragione del ruolo rivestito all'interno dell'amministrazione comunale, oppure delle funzioni svolte.

2. I soggetti in parola devono rispettare le seguenti istruzioni:

● trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;

● verificare la legittimità e correttezza dei trattamenti, valutando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere;

- Verificare che i trattamenti avvengano nel rispetto delle policy adottate dal Comune in materia di sicurezza, logistica e informatica, e di protezione dei dati personali.

3. Sono, altresì, designati al trattamento tutti i soggetti, dipendenti e collaboratori a qualsiasi titolo che operano sotto la diretta autorità dei Responsabili esterni del trattamento ed effettuano operazioni di trattamento.

4. Gli incaricati sono quindi designati / autorizzati per iscritto:

- tramite individuazione nominativa (nome e cognome) delle persone fisiche, con specifica indicazione dei trattamenti affidati;

- tramite assegnazione funzionale della persona fisica alla unità organizzativa di minori dimensioni, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.

La designazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento con riguardo anche ad eventuali aspetti di dettaglio relativi alle specificità dei singoli trattamenti.

Art.8
Sicurezza del trattamento

1. Il Comune di Monte Romano e ciascun Responsabile del trattamento mettono 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, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche e organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la minimizzazione delle attività di trattamento; la pseudonimizzazione o 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.

3. Costituiscono misure tecniche e organizzative che, una volta adottate, devono essere applicate e monitorate dal Servizio cui è preposto ciascun Responsabile del trattamento:

- sistemi di autenticazione, sistemi di autorizzazione, sistemi di protezione (antivirus, firewall, antintrusione, altro), utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche;
- misure antincendio, sistemi di rilevazione di intrusione, sistemi di sorveglianza, 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.

Il Comune di Monte Romano e ciascun Responsabile del trattamento impartiscono appropriate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

4. Per quanto riguarda il Comune di Monte Romano, la conformità del trattamento dei dati al GDPR è dimostrata attraverso la predisposizione e approvazione di un apposito documento che definisce le misure di sicurezza da applicare e le procedure da osservare per garantire la protezione dei dati personali nell'ambito delle attività di trattamento effettuate e il corretto adempimento degli obblighi posti in capo al Titolare dalla normativa europea e nazionale di riferimento; il documento in parola individua e formalizza un modello organizzativo - gestionale, sul cui costante aggiornamento e sulla cui effettiva ed efficace implementazione all'interno dell'amministrazione comunale il Titolare e, per esso – negli ambiti e nei limiti di rispettiva competenza – i Responsabili (interni) del trattamento, sono chiamati a vigilare, anche con il supporto del Responsabile della protezione dei dati personali.

5. Le disposizioni del presente regolamento si intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'esterno. L'accesso ai dati personali da parte delle strutture e dei dipendenti del comune comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale il comune provvede alla organizzazione

delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitare l'accesso e la fruizione, anche presso le strutture dipendenti.

Ogni richiesta di accesso ai dati personali da parte delle strutture e dei dipendenti comunali, debitamente motivata, deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale.

Il responsabile della banca dati, specie se la comunicazione concerne dati sensibili, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone.

6. I nominativi ed i dati di contatto del Titolare, dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "GDPR".

7. Restano in vigore le misure di sicurezza previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico, nel rispetto degli specifici regolamenti attuativi, adottate nel vigore della precedente disciplina normativa (ex artt. 20 e 22, D.Lgs. n. 193/2006).

Art. 9
Coordinamento con amministrazione trasparente, procedimenti di accesso civico, generalizzato e documentale

1. Costituisce onere sia del R.P.D. che del Responsabile Comunale per la prevenzione della corruzione e della trasparenza coordinare la loro attività al fine di semplificare e minimizzare l'impatto degli adempimenti sull'attività degli uffici e garantire la massima protezione dei dati personali ogniqualvolta procedimenti di ufficio o attivati su istanza di soggetti esterni comportino attività di pubblicazione dei dati personali in amministrazione trasparente, il rilascio di dati personali in occasione di istanze di accesso civico, generalizzato e documentale.

2. In tali ultime ipotesi dovranno essere adottate misure di sicurezza adeguate, compresa la minimizzazione e la pseudonimizzazione oppure cifratura dei dati personali.

3. Il R.P.D., se interpellato, svolge le funzioni di supporto alle strutture competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato.

4. Il R.P.D. svolge altresì le funzioni di supporto al Responsabile Comunale per la prevenzione della corruzione e della trasparenza nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali.

5. Il R.P.D., inoltre, su richiesta delle strutture, esprime proprio parere in ordine alla valutazione dell'eventuale pregiudizio che l'accesso potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016. Il R.P.D., su richiesta delle strutture, formula il proprio parere, entro tre giorni, in ordine all'opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti: sulla scorta di tale parere le strutture competenti sulle singole

richieste di accesso effettueranno il bilanciamento tra gli interessi asseritamente lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.

Art. 10
Formazione del personale

1. Costituisce onere sia del Responsabile comunale della protezione dei dati personali che del Responsabile Comunale per la prevenzione della corruzione e della trasparenza coordinare la loro attività al fine di attuare misure di formazione del personale, anche con riscontro dell'acquisizione di abilità e competenze, al fine di garantire, nell'attività degli uffici, il rispetto delle norme in materia di trasparenza e l'assolvimento degli adempimenti atti a tutelare i diritti di riservatezza dei dati personali dei cittadini e dipendenti.

Art. 11
Trattamenti consentiti.

1. Il Comune, di norma, non è tenuto a chiedere il consenso al trattamento dei dati da parte degli interessati.
2. La pubblicazione e la divulgazione di atti e documenti che determinano una "diffusione" dei dati personali, comportando la conoscenza dei dati da parte di un numero indeterminato di cittadini, è legittima solo se la diffusione è prevista da una norma di legge o di regolamento.
3. Prima della pubblicazione di dati personali deve essere valutato se le finalità di trasparenza e di comunicazione possono essere perseguite senza divulgare dati personali.
4. Se risulta possibile occorre citare i dati personali solo negli atti a disposizione degli uffici, richiamati quale presupposto della deliberazione e consultabili solo da interessati e contro interessati oppure utilizzare espressioni di carattere generale, soprattutto nel quadro dell'attività di assistenza e beneficenza, che spesso comporta la valutazione di circostanze e requisiti personali che attengono a situazioni di particolare disagio.
5. Deve essere valutato anche la possibilità di rendere pubblici atti e documenti senza indicare i dati che portino all'identificazione degli interessati.
6. Per attività di comunicazione istituzionale che contemplino l'utilizzo di dati personali, andrà posta particolare attenzione alla necessità di fornire un'adeguata informativa relativa al trattamento e soprattutto andrà valutato se risulti necessaria l'acquisizione, anche successivo, del consenso al trattamento.
7. 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, rispettando il principio di proporzionalità, mediante la verifica che tale pubblicazione a fini di trasparenza concerne solo dati pertinenti e non eccedenti rispetto alle finalità perseguite.
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 estratti degli atti con l'esclusione dei dati personali in essi contenuti.

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

9. 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 alla loro nomina, al percorso professionale e ai fatti più significativi che li riguardano, possono mantenere la loro unitarietà, adottando accorgimenti che impediscano un accesso indiscriminato, quali l’utilizzo di sezioni o fascicoli dedicati alla custodia di eventuali dati sensibili, da conservare chiusi o comunque con modalità che riducano la possibilità di una indistinta consultazione nel corso delle ordinarie attività amministrative.

Art. 12
Trattamento e accesso ai dati particolari e relativi a condanne penali e reati

1. Per l’accesso ai dati particolari o ai dati relativi a condanne penali e reati, con determinazione del Responsabile del Settore e/o decreto sindacale sono rilasciate autorizzazioni singole o a gruppi di lavoro per il trattamento dei dati.

2. L’autorizzazione è limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni assegnate all’incaricato.

3. In attuazione del Regolamento UE 2016/679, si indicano di seguito le categorie di dati di cui è consentito il trattamento per specifiche finalità di rilevante interesse pubblico perseguite dal Comune nello svolgimento delle proprie attività istituzionali:

1) Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune;

2) Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - Attività relativa al riconoscimento di benefici connessi all'invalidità civile e all'invalidità derivante da cause di servizio, nonché da riconoscimento di inabilità a svolgere attività lavorativa;

3) Servizi demografici / Anagrafe - Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE);

4) Servizi demografici / Stato civile - Attività di gestione dei registri di stato civile;

5) Servizi demografici / Elettorale - Attività relativa all'elettorato attivo e passivo;

6) Servizi demografici / Elettorale - Attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio;

7) Servizi demografici / Elettorale - Attività relativa alla tenuta dell'elenco dei giudici popolari;

8) Servizi demografici/DAT – Attività connesse alle Disposizioni anticipate di trattamento;

9) Servizi demografici / Leva - Attività relativa alla tenuta del registro degli obiettori di coscienza;

10) Servizi demografici / Leva - Attività relativa alla tenuta delle liste di leva e dei registri matricolari;

11) Servizi sociali - Attività relativa all'assistenza domiciliare;

12) Servizi sociali - Attività relativa all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale;

13) Servizi sociali - Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, RSA ecc.;

14) Servizi sociali - Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale;

15) Servizi sociali - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali);

16) Servizi sociali - Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.);

17) Servizi sociali - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto;

18) Servizi sociali - Attività relativa alla prevenzione ed al sostegno alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno);

19) Servizi sociali - Attività relativa ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori;

20) Servizi sociali - Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.);

21) Servizi sociali - Attività relative alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario;

22) Istruzione e cultura - Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne, elementari e medie;

23) Istruzione e cultura - Attività di formazione ed in favore del diritto allo studio;

24) Istruzione e cultura - Gestione delle biblioteche, archivi storici e dei centri di documentazione;

25) Polizia municipale - Attività relativa all'infortunistica stradale;

26) Polizia municipale - Gestione delle procedure sanzionatorie;

27) Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, in materia di commercio e attività produttive nonché di polizia mortuaria;

28) Polizia municipale - Attività relativa al rilascio di permessi per invalidi;

29) Polizia municipale – Attività connesse all’utilizzo degli impianti di videosorveglianza di proprietà comunale dislocati sul territorio comunale;

30) SUAP - Rilascio autorizzazioni in materia di commercio, pubblici esercizi, artigianato, attività produttive e di pubblica sicurezza;

31) Avvocatura - Attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione, nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione;

32) Politiche del lavoro - Gestione delle attività relative all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale;

33) Gestione dei dati relativi agli organi istituzionali dell'ente, del difensore civico regionale, nonché dei rappresentanti dell'ente presso enti, aziende e istituzioni;

34) Attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali;

35) Attività connesse alla richieste del difensore civico regionale;

36) Attività riguardante gli istituti di democrazia diretta;

37) Attività di protezione civile;

38) Conferimento di onorificenze o ricompense;

39) Agevolazioni tributarie;

40) Attività ricreative, promozione della cultura e dello sport - occupazione di suolo pubblico - uso di beni mobili ed immobili comunali;

41) Iscrizioni ad albi comunali di associazioni ed organizzazioni di volontariato.

4. I dati particolari o relativi a condanne penali e reati individuati dal presente Regolamento sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'interessato.

5. I dati non indispensabili di cui il Comune, nell'espletamento della propria attività istituzionale, venga a conoscenza, per via dell'attività dell'interessato, non sono utilizzati in alcun modo; salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Art.13
Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto del Comune, del Sindaco e/o del suo Delegato ai sensi del precedente art. 2, eventualmente del Contitolare del trattamento, del RPD;
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, come da precedente art. 8.

2. Il Registro si compone di diverse “schede” (fogli excel), ciascuna associata ad uno specifico Settore /Area di operatività, secondo lo schema di cui all’allegato A, e di una scheda riepilogativa finale, secondo lo schema di cui all’allegato C al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell’Ente. Il Registro è conservato presso gli uffici della struttura organizzativa del Comune in formato elettronico.

3. Il Registro è tenuto e aggiornato dal Titolare con la collaborazione e il supporto dei Responsabili del trattamento designati ai sensi del precedente art. 5, ciascuno per quanto di rispettiva competenza.

4. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere e aggiornare il Registro, sotto la responsabilità del medesimo Titolare.

5. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Art.14
Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Responsabile (esterno) di cui al precedente art. 5, reca le seguenti informazioni:

a) il nome ed i dati di contatto del Responsabile del trattamento e dell’eventuale RPD;
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, come da precedente art. 7.

2. Il registro, predisposto secondo lo schema di cui all’allegato B al presente Regolamento, è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea.

3. Il Responsabile del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.

Art. 15
Valutazioni d’impatto sulla protezione dei dati

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, prima di effettuare il trattamento, deve attuare una valutazione dell’impatto del medesimo trattamento (DPIA) ai sensi dell’art.

35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante ai sensi dell'at. 35, pp. 4-6, GDPR.

3. La DPIA è 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, 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 particolari o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del 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.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.

Il Titolare deve 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 della DPIA. Il RPD monitora lo svolgimento della DPIA.

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

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 DPIA.

5. 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.

6. 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 DPIA. In questo caso si possono utilizzare i risultati della DPIA 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 DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. 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.

7. La DPIA 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;
- della consultazione preventiva del Garante;

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.

8. 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.

9. Il Titolare deve consultare il Garante 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.

10. 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. 16
Violazione dei dati personali

1. 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. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

2. 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).

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, 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).

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

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

Art. 17
Diritti dell'interessato

1. I soggetti, i cui dati sono contenuti in una banca dati del comune, hanno il diritto di ottenere, senza indugio:

a) la conferma dell'esistenza o meno di trattamenti di dati che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché

della logica e delle finalità del trattamento;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
c) l'aggiornamento, la rettificazione, ovvero, qualora vi abbia interesse, l'integrazione dei dati;
d) l'attestazione che le operazioni di cui ai successivi commi 2 e 3 sono state portate a conoscenza dei terzi;
e) la disponibilità dei dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico per trasmetterli a un altro titolare del trattamento.

2. L'interessato ha, inoltre, il diritto di opporsi, per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta.

3. L'interessato può esercitare tali diritti con una richiesta al Titolare, oppure ai Responsabili del Trattamento, oppure al Responsabile della protezione dei dati personali, avvalendosi della apposita modulistica presente nella sezione "privacy" del Sito istituzionale del Comune.

4. L'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

Art.18
Rinvio

1. Per tutto quanto non espressamente disciplinato nel presente Regolamento si applicano le disposizioni del GDPR, del Decreto Legislativo 30 giugno 2003 n. 196, come modificato e integrato dal Decreto Legislativo 10 agosto 2018, n. 101, e tutte le altre disposizioni e previsioni vigenti in materia di trattamento e protezione dei dati personali.

2. Le norme del presente regolamento si intendono modificate per effetto di sopravvenute norme vincolanti comunitarie per la parte direttamente applicabile, statali e regionali; in tali casi, in attesa della formale modificazione del presente regolamento, si applica la normativa sopraordinata.

Art. 19
Pubblicità del regolamento

1. Copia del presente regolamento è pubblicato nell'apposita sezione "*GDPR*" e/o in *Amministrazione trasparente* del Sito internet istituzionale.