



Comune di Calatabiano

Città Metropolitana di Catania

Piazza Vittorio Emanuele, 32
95011 Calatabiano (CT) - Italy
Tel. 095 7771037 - Fax 095 7771080
Codice Fiscale: 00462070871
Email: protocollo@pec.comune.calatabiano.ct.it

Regolamento per la gestione della riservatezza dei dati personali

Regolamento approvato con deliberazione di Consiglio Comunale n. 13 del 25.02.2019

Regolamento per la gestione della riservatezza dei dati personali

SOMMARIO	
Art. 1 - Oggetto del regolamento	4
Art. 2 - Finalità	4
Art. 3 - Definizioni	5
Art. 4 – Soggetti	6
Art. 5 - Responsabile della protezione dei dati	7
Art. 6 – Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati comunali e valutazione di impatto sulla protezione dei dati	8
Art. 7 - Trattamento dei dati personali	8
Art. 8 – Coordinamento con amministrazione trasparente, procedimenti di accesso civico, generalizzato e documentale	8
Art. 9 - Formazione ed informazione del personale	8
Art. 10 – Trattamenti consentiti.	9
Art. 11 - Principi	9
Art. 12 - Attività amministrativa	9
Art. 13. - Fascicolo personale dipendenti e amministratori	9
Art. 14 - Sicurezza dei dati – Misure di sicurezza – Verifiche e controlli	10
Art. 15 – Trattamento e accesso a categorie particolari di dati (“dati sensibili”) e giudiziari	11

Regolamento per la gestione della riservatezza dei dati personali

Art. 16 – Registro delle attività di trattamento	11
Art. 17 - Diritti dell'interessato	11
Art. 18 – Valutazione d'impatto sulla protezione dei dati	12
Art. 19 – Entrata in vigore e normativa applicabile	14
Art. 20 - Rinvio dinamico	14
Art. 21 - Norme abrogate	14
Art. 22 - Pubblicità del regolamento	15

Art. 1 - Oggetto del regolamento

1. Il presente regolamento disciplina il trattamento dei dati personali contenuti nelle banche dati organizzate, gestite od utilizzate dall'amministrazione, in relazione allo svolgimento delle proprie finalità istituzionali, in attuazione:
 - della normativa in materia di diritto di accesso documentale, accesso civico e accesso generalizzato;
 - del Regolamento UE 2016/679 del 27 aprile 2016 relativo alla *“protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”* e che abroga la direttiva 95/46/CE;
 - del Decreto Legislativo 18 maggio 2018, n. 51;
 - del Decreto Legislativo 10 agosto 2018, n. 101 - *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.*

Art. 2 - Finalità

1. L'Unione, nell'assolvimento delle proprie finalità istituzionali secondo i principi di trasparenza, efficacia ed economicità ed in adempimento dell'obbligo di comunicazione interna ed esterna e di semplificazione dell'azione amministrativa:
 - garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il rispetto del diritto alla riservatezza ed all'identità personale nonché delle norme vigenti in materia di protezione e gestione dei dati;
 - 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 nell'ambito dell'Unione Europea.
2. 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 dalle leggi, dallo statuto e dai regolamenti o per effetto di accordi e/o convenzioni.
4. I trattamenti sono compiuti dal Comune per le seguenti finalità:
 - a) 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 all'Unione in base alla vigente legislazione.*
 - b) adempimento di un obbligo legale al quale è soggetta l'Unione. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
 - c) esecuzione di un contratto con soggetti interessati.

Regolamento per la gestione della riservatezza dei dati personali

Art. 3 - 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) **"Categorie particolari di dati ("dati sensibili" e "giudiziari")"**: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché la trattazione di 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;
- e) **"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;
- f) **"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;
- g) **"Terzi o incaricati"**: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- h) **"Interessato"**: la persona fisica, cui si riferiscono i dati personali;
- i) **"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;
- j) **"Dato anonimo"**: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- k) **"Blocco"**: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- l) **"Banca di dati"**: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- m) **"Garante"**: l'autorità preposta al controllo della privacy;
- n) **"Violazione di dati personali"**: 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;
- o) **"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;

- p) **"Pseudonimizzazione"**: *il trattamento dei dati personali in modo tale che i dati personali 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. 4 – Soggetti

1. Il Comune di Calatabiano, rappresentato, in ossequio al Regolamento UE 2016/679, dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco può delegare le relative funzioni ad un Responsabile di P.O. in possesso di adeguate competenze.
2. Il Titolare è responsabile del rispetto dei principi contenuti nell'art. 5 del Regolamento UE 2016/679:
 - liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare adotta misure appropriate per fornire all'interessato:
 - a) le informazioni indicate dall'art. 13 del Regolamento UE 2016/679, qualora i dati personali siano raccolti presso lo stesso interessato;
 - b) le informazioni indicate dall'art. 14 del Regolamento UE 2016/679, qualora i dati personali non siano 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 del Regolamento citato, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento e tenuto conto di quanto indicato dal successivo art. 9.
5. Il Titolare, inoltre, provvede a:
 - a) **designare** i Responsabili del trattamento nelle persone dei Responsabili di P.O. 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. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;
 - b) **nominare** il Responsabile della protezione dei dati "DP.O.";
 - c) **nominare** quale Responsabile del trattamento 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. Il Responsabile del trattamento, designato mediante determinazione del Sindaco, 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 a:
 - a) tenere il registro delle categorie di attività di trattamento svolte per conto del Titolare;
 - b) adottare idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
 - c) assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati

Regolamento per la gestione della riservatezza dei dati personali

fornendo allo stesso ogni informazione di cui è in possesso;

- d) informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (c.d. *"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.

Art. 5 - Responsabile della protezione dei dati

1. Il Sindaco, con suo provvedimento, nomina il Responsabile della protezione dei dati, in funzione delle sue qualità professionali ed, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti di controllo a lui affidati.
2. Il Responsabile della protezione dei dati può essere un funzionario/dipendente in posizione apicale oppure un incaricato esterno che potrà assolvere i suoi compiti in base a un contratto di servizio.
3. I dati di contatto del Responsabile della protezione dei dati sono pubblicati sul sito istituzionale del Comune, nella sezione *"Amministrazione trasparente"* e comunicati al Garante della protezione dei dati personali.
4. Il Responsabile della protezione dei dati deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
5. Al Responsabile della protezione dei dati vanno fornite le risorse necessarie per assolvere i propri compiti, accedere ai dati personali, ai trattamenti e per mantenere la propria conoscenza specialistica. Questi non può essere rimosso o penalizzato a causa dell'adempimento di detti compiti. Riferisce e dipende direttamente al Sindaco o ad un suo delegato ed ai Responsabili nominati.
6. I cittadini/utenti possono contattare il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
7. Il Responsabile della protezione dei dati è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti ed, in conformità del diritto dell'Unione o degli Stati membri, deve svolgere almeno le seguenti funzioni:
 - a) sorvegliare l'osservanza del presente regolamento nonché della normativa nazionale e comunitaria da parte dei titolari del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
 - b) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
 - c) cooperare con l'Autorità garante per la protezione dei dati personali e fungere da punto di contatto per questioni connesse al trattamento dei dati personali;
 - d) informare e fornire consulenza al consiglio, alla giunta, al sindaco e agli assessori e a tutti gli uffici comunali in merito agli obblighi derivanti dal presente regolamento nonché dalla normativa nazionale e comunitaria.
8. I compiti attribuiti al DPO sono indicati in apposito contratto di servizi. L'incarico di DPO può essere affidato anche ad un unico soggetto designato da più Comuni mediante esercizio associato della funzione nelle forme previste dal D.Lgs. 18 agosto 2000 n. 267.

Art. 6 – Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati comunali e valutazione di impatto sulla protezione dei dati

1. Al fine di coordinare le attività oggetto di trattamento, è utilizzato il “**Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati comunali e valutazione di impatto sulla protezione dei dati**”.
2. Il Responsabile della protezione dei dati personali dà un termine a ciascuna posizione organizzativa per aggiornare e compilare le schede afferenti alle banche dati affidate alla gestione di detti soggetti.
3. La conformità del trattamento dei dati al Regolamento in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta.

Art. 7 - Trattamento dei dati personali

1. 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.
2. Ogni richiesta di accesso ai dati personali da parte delle strutture e dei dipendenti dell'Ente, debitamente motivata, deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale.
3. 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.

Art. 8 – Coordinamento con amministrazione trasparente, procedimenti di accesso civico, generalizzato e documentale

1. Costituisce onere, sia del **Responsabile della protezione dei dati personali** che del **Responsabile 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 pseudonimizzazione, la minimizzazione e la cifratura dei dati personali.

Art. 9 - Formazione ed informazione del personale

1. Costituisce onere sia del **Responsabile della protezione dei dati personali** che del **Responsabile Comunale per la prevenzione della corruzione e della trasparenza**, nel caso in cui siano incaricati due soggetti diversi, coordinare la loro attività al fine di attuare misure di formazione ed informazione 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.

Regolamento per la gestione della riservatezza dei dati personali

Art. 10 – 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 controinteressati 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 valutata 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 successiva, del consenso al trattamento.

Art. 11 - Principi

1. 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.
2. 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.

Art. 12 - Attività amministrativa

1. L’attività amministrativa del Comune si svolge, principalmente, con l’emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.
2. Per l’attività informatica di cui al comma precedente sono rigorosamente rispettate le norme del codice dell’amministrazione digitale approvato con decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni ed integrazioni.
3. La sicurezza dei dati personali è assicurata anche mediante adeguate soluzioni tecniche connesse all’utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche.

Art. 13. - Fascicolo personale dipendenti e amministratori

1. I dati sullo stato di salute dei dipendenti e degli amministratori devono essere conservati separatamente rispetto alle altre informazioni personali. Il fascicolo, che raccoglie tutti gli atti relativi 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. 14 - Sicurezza dei dati – Misure di sicurezza – Verifiche e controlli

1. Tutta l'attività di gestione è finalizzata a:
 - a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati;
 - b) evitare l'accesso, non autorizzato, alle banche dati, alla rete ed, in generale, ai servizi informatici del Comune;
 - c) prevenire:
 - trattamenti dei dati non conformi alla legge o ai regolamenti;
 - la cessione o la distribuzione dei dati in caso di cessazione del trattamento.
2. I Responsabili del trattamento e delle banche dati garantiscono, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, l'adozione e lo sviluppo di misure di sicurezza adeguate come:
 - la pseudonimizzazione;
 - la minimizzazione;
 - la cifratura dei dati personali;
 - la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
 - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
 - una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Nella gestione dei dati personali con il sistema informatizzato dovrà essere assicurato il puntuale e scrupoloso rispetto di tutte le norme vigenti.
4. Gli stessi responsabili delle banche dati si attiveranno periodicamente con controlli, anche a campione, al fine di garantire la sicurezza delle banche dati e la esattezza e completezza dei dati inseriti.
5. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:
 - *sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);*
 - *misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.*
6. Ogni ulteriore misura idonea a tutela delle banche dati personali informatiche o cartacee andrà adottata secondo un principio di proporzionalità tra le risorse disponibili e i diritti da tutelare.

Art. 15 – Trattamento e accesso a categorie particolari di dati (“dati sensibili”) e giudiziari

1. Per l'accesso a categorie particolari di dati (“dati sensibili” e “dati giudiziari”, con determinazione del Responsabile del servizio sono rilasciate autorizzazioni singole o a gruppi di lavoro per il trattamento dei dati e la manutenzione.
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, *il Registro dei Trattamenti* identifica i tipi di dati per cui è consentito il relativo trattamento.
4. I suddetti dati individuati 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, dei quali il Comune, nell'espletamento della propria attività istituzionale, venga a conoscenza, ad opera dell'interessato e comunque non a richiesta del Comune medesimo, non sono utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Art. 16 – 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. 4, eventualmente del Contitolare del trattamento e del D.P.O;*
 - 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.6.*
2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 4, presso gli uffici della struttura organizzativa del Comune, in forma telematica/cartacea, secondo quanto previsto dal Regolamento UE; nello stesso, possono essere inserite ulteriori informazioni ritenute utili tenuto conto delle dimensioni organizzative dell'Ente.

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 li 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 siano state portate a conoscenza dei terzi.
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 responsabile della banca dati.
4. L'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

Art. 18 – Valutazione 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 – Data Protection Impact Analysis (**DPIA**) ai sensi dell'art. 35 del Regolamento UE, 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 Privacy ai sensi dell'art. 35 del Regolamento UE.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Ferma restando quanto indicato dall'art. 35, p. 3, del Regolamento UE, 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 analogo natura ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;*
 - c) *monitoraggio sistematico ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;*
 - d) *trattamenti di dati sensibili o dati di natura estremamente personale ossia le categorie particolari di dati personali di cui all'art. 9 del Regolamento UE;*
 - e) *trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;*
 - f) *combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;*
 - g) *dati relativi a interessati vulnerabili ossia ad 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;*
 - b) *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.*