

# **Città di Policoro**



**REGOLAMENTO COMUNALE PER  
L'ATTUAZIONE DEL REGOLAMENTO UE  
2016/679 RELATIVO ALLA PROTEZIONE  
DELLE PERSONE FISICHE CON RIGUARDO AL  
TRATTAMENTO DEI DATI PERSONALI**

**Art. 1 - Oggetto**

**Art. 2 - Definizioni**

**Art. 3 - Titolare del trattamento**

**Art. 4 - Soggetto Designato al Trattamento dei Dati Personali**

**Art. 5 - Responsabile (Esterno) del Trattamento dei Dati Personali**

**Art. 6 - Sub-Responsabile del Trattamento dei Dati Personali**

**Art. 7 - Persona Autorizzata al Trattamento (PAT)**

**Art. 8 - Amministratore Di Sistema (ADS)**

**Art. 9 - Finalità del trattamento**

**Art. 10 - Diritti degli interessati**

**Art. 11 -Responsabile della Protezione dei Dati**

**Art. 12 - Sicurezza del trattamento**

**Art. 13 -Registro delle attività di trattamento**

**Art. 14 - Obbligo di informativa**

**Art. 15 - Valutazione d'impatto sulla protezione dei dati**

**Art. 16 - Violazione dei dati personali**

**Art. 17 - Rinvio**

**Allegati**

**A) schema di registro attività di trattamento**

**B) schema di registro categorie attività di trattamento**

## **Art. 1** **Oggetto**

1. Il presente Regolamento ha per oggetto misure procedurali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Policoro. Ai sensi dell'art. 5 del GDPR, i dati personali oggetto di trattamento devono essere:

- a) *trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;*
- b) *raccolti e trattati per finalità determinate, esplicite e legittime;*
- c) *adeguati, pertinenti e limitati alle finalità per le quali sono trattati;*
- d) *esatti e, se necessario, aggiornati;*
- e) *conservati in modo da consentirne l'identificazione degli interessati per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono trattati;*
- f) *trattati in maniera da garantirne un'adeguata sicurezza.*

## **Art.2** **Definizioni**

Ai fini del presente Regolamento, si intende per:

- a) **Titolare del trattamento:** il Comune di Policoro, in quanto soggetto che unitariamente determina finalità e mezzi del trattamento di dati personali.
- b) **Soggetto Designato:** il/la Dirigente o Responsabile espressamente designato/a ai sensi dell'art2-*quaterdecies* D.lgs. 196/2003, al/alla quale sono attribuiti specifici compiti e funzioni relativi al trattamento dei dati personali.
- c) **Soggetti Autorizzati (PAT):** personale opportunamente istruito e nominato ai sensi dell'art. 29 GDPR che ha accesso ai dati personali ed opera sotto l'autorità del Titolare del Trattamento.
- d) **Responsabile del trattamento:** 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 idoneamente designato ai sensi dell'art. 28 GDPR.

- e) **Sub-Responsabile del trattamento:** soggetto incaricato dal Responsabile del trattamento ai sensi dell'art. 28 GDPR per l'esecuzione di specifiche attività di trattamento svolte per conto del Titolare del trattamento.
- f) **Contitolare:** qualunque soggetto, pubblico o privato, con il quale il Titolare del trattamento intrattiene un rapporto di contitolarità ai sensi dell'art. 26 GDPR riferito ad uno specifico trattamento il cui fine ed i mezzi sono congiuntamente determinati.
- g) **Amministratore di Sistema (ADS):** figura professionale essenziale per la sicurezza delle banche dati e la corretta gestione delle reti telematiche; è un esperto chiamato a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali; a lui viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informativi aziendali o di una pubblica amministrazione.
- h) **Responsabile per la protezione dati (DPO):** il/la dipendente della struttura organizzativa del Titolare, il professionista privato o impresa esterna, incaricato ai sensi dell'art. 37 GDPR.
- i) **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (*interessato/a*) attraverso, ad esempio, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale, ai sensi dell'art. 4 par. 1 GDPR.
- j) **Registro delle attività di trattamento del Titolare del trattamento:** insieme dei Registri dei trattamenti di Settore tenuti in forma telematica da ciascun/ciascuna Dirigente Capo Settore secondo le rispettive competenze e contenenti gli elementi richiesti all'art. 30 GDPR.
- k) **Valutazione d'impatto sulla protezione dei dati (DPIA):** procedura finalizzata a descrivere un trattamento comportante un rischio elevato, e a valutarne necessità e proporzionalità, e facilitare la gestione e la prevenzione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali, ai fini di dimostrarne la conformità rispetto alle previsioni normative.
- l) **Violazione di dati personali / Data breach:** qualsiasi violazione di sicurezza accertata o in corso di accertamento che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati.

- m) **Garante:** Garante per la Protezione dei Dati Personali istituito dalla Legge 31 dicembre 1996 n. 675, quale Autorità amministrativa pubblica di controllo indipendente.

### **Art. 3**

#### **Titolare del trattamento**

1. Il Comune di Policoro, rappresentato ai fini previsti dal RGPD dal Sindaco pro-tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee. Il Sindaco può delegare con **decreto sindacale** le relative funzioni a Dirigente/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 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. 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 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.

4. Il Titolare adotta misure appropriate per fornire all'interessato:
  - a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
  - b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (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. 9.

6. Il Titolare, inoltre, provvede a:

a) nominare il Soggetto Designato al Trattamento nelle persone dei Dirigenti/Responsabili P.O. e dei Funzionari delle singole strutture 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.

b) nominare il Responsabile della protezione dei dati (DPO);

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;

d) predisporre l'elenco dei **Soggetti Designati al Trattamento** delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

7. 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 RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

8. 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 RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

## **A. Principio di “Accountability”**

In base al principio di responsabilizzazione (accountability), introdotto dal GDPR e dal d.lgs. 10 agosto 2018, n. 101 il Titolare del trattamento si deve responsabilizzare autonomamente nella gestione ed organizzazione della Privacy. Il principio nasce nella legislazione europea e statunitense ed è inteso come la responsabilità dell'amministrazione che ha verso chi l'ha scelta e si fonda su:

1. trasparenza intesa come informazioni dell'attività di governo;
2. partecipazione di chiunque al miglioramento delle politiche pubbliche;
3. collaborazione intesa come efficacia dell'azione amministrativa attraverso la cooperazione tra tutti i livelli di governo;

**B. Il Titolare del trattamento** è il soggetto al quale è imputata l'*accountability* (“responsabilizzazione”), nella sua duplice accezione:

**Responsabilità:** il Titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire che il trattamento è effettuato in conformità alle disposizioni regolamentari *“tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche”*.

**Verificabilità:** il Titolare deve poter dimostrare la conformità (inversione dell'onere della prova).

Il Titolare è l'Ente nel suo complesso e nel caso di specie il Comune di Policoro.

All'interno di una struttura organizzativa così complessa, il Titolare del trattamento, nella persona del legale rappresentante, delega specifici compiti o funzioni a soggetti interni alla propria organizzazione, in considerazione dell'impossibilità di gestire singolarmente l'adozione delle misure di sicurezza previste e l'osservanza degli adempimenti prescritti. Pertanto:

- tenuto conto del contesto organizzativo dell'Ente/Comune;
- in coerenza con l'assetto organizzativo proprio dell'Ente che si compone di nr. 5

Settori e la Struttura Autonoma Complessa di Polizia Locale:

1. Settori I - Amministrativo;
2. Settori II – Ragioneria, Finanza e Affari Personali;
3. Settori III - Tecnico;
4. Settori IV – SUAP e Polizia Amministrativa;
5. Settori V – Tecnico e Manutenzione;
6. Staff Sindaco – Polizia Locale;

- considerati i ruoli strategici e di responsabilità delle diverse Aree e Uffici;
- in coerenza con il sistema di gestione privacy definito;

Si individuano compiti e funzioni potenzialmente delegabili, ordinariamente o straordinariamente, dal Titolare del trattamento/rappresentante legale ai responsabili dei Settori/Aree, in base ai seguenti parametri quantitativi e qualitativi:

- complessità e valore dello specifico compito o funzione;
- programmazione delle attività operative;
- eterogeneità dei trattamenti eseguiti;
- prevedibilità e probabilità del verificarsi di un evento;
- necessità di controllo e monitoraggio continuo;
- esigenze organizzative interne;
- quantità del personale autorizzato al trattamento;
- continuità rispetto ad un precedente sistema di gestione privacy.

#### **FUNZIONI E COMPITI CHE PERMANGONO ORDINARIAMENTE IN CAPO AL TITOLARE:**

- ✓ Determinazione delle finalità e delle modalità del trattamento.
- ✓ Individuazione delle misure di sicurezza tecniche ed organizzative adeguate.
- ✓ Adozione delle misure tecniche ed organizzative adeguate per la protezione dei dati personali.

#### **FUNZIONI E COMPITI ORDINARIAMENTE DELEGABILI:**

- ✓ Individuazione e designazione dei Responsabili (esterni) del trattamento.
- ✓ Individuazione e designazione delle Persone Autorizzate al trattamento (PAT).
- ✓ Formazione delle Persone Autorizzate al Trattamento (PAT).
- ✓ Predisposizione e comunicazione delle istruzioni a soggetti designati e PAT.
- ✓ Tenuta e aggiornamento del Registro delle attività di trattamento.
- ✓ Tenuta e aggiornamento del Registro delle violazioni.
- ✓ Tenuta e aggiornamento del Registro delle informative.
- ✓ Vigilanza sulla corretta applicazione delle misure tecniche ed organizzative per la protezione dei dati personali.
- ✓ Attività di valutazione del rischio e/o valutazioni di impatto (DPIA).
- ✓ Individuazione e designazione dell'Amministratore di sistema (ADS).

## **FUNZIONI E COMPITI STRAORDINARIAMENTE DELEGABILI:**

- Notifica di violazione dei dati personali (data breach) all'Autorità Garante, nei casi previsti dal Regolamento.
- Comunicazione di violazione dei dati personali (data breach) all'interessato, nei casi previsti dal Regolamento.
- Comunicazione del DPO/RPD all'Autorità nazionale di controllo (Garante per la protezione dei dati personali).

I suddetti compiti/funzioni possono essere attribuiti dal Titolare del trattamento a persone fisiche interne alla propria organizzazione in maniera **verticale** o **orizzontale** (trasversale), tenendo conto anche della **specialità del soggetto designato** (delegato).

La **delega di funzione orizzontale** si sostanzia nell'attribuzione di compiti o funzioni trasversali per tutto il personale delle varie strutture o per tutte le strutture stesse dell'Ente.

La **delega di funzione verticale** si sostanzia, invece, nell'affidamento di compiti o funzioni verticali a persone fisiche che ricoprono il ruolo di **Dirigenti/Responsabili di Aree/Settori**, dato che agli stessi sono riconosciuti: ampia autonomia organizzativa, gestionale ed operativa con piena assunzione di responsabilità per il raggiungimento degli obiettivi prestazionali e di qualità definiti.

In ambito privacy la delega verticale prevede il conferimento di più compiti e più funzioni, di competenza del Titolare del trattamento, finalizzate a promuovere l'impegno e l'attiva partecipazione alla realizzazione del sistema di gestione privacy implementato.

### **Art. 4**

#### **Soggetto Designato al Trattamento dei Dati Personali**

L'art. 2-*quaterdecies* del D. Lgs. 196/2003, novellato dal D. Lgs. 101/2018, come detto, stabilisce che *“il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità”* (co. 1). Inoltre, al co. 2, è specificato che *“il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta”*. Il **Soggetto Designato** è dunque il destinatario della

facoltà di delega, orizzontale o verticale, del Titolare del trattamento e diviene figura fondamentale di coordinamento interno all'organizzazione dell'Ente.

I dipendenti del Comune sono designati, di norma, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

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

Il Soggetto **designato 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), 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 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 (Esterno) del Trattamento dei Dati Personali**

Il **Responsabile del trattamento** è *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento"* (art. 4 GDPR). Si tratta di una figura designata dal Titolare, mediante contratto o altro atto giuridico, e legittimata ad operare per suo conto, purché presti *"garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate"* a garantire la tutela dei diritti e delle libertà fondamentali dell'interessato.

Il contratto o l'atto giuridico di designazione, stipulato in forma scritta, specifica 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.

Inoltre, tale contratto o atto giuridico di designazione vincola il Responsabile, a norma dell'art.28 GDPR a:

- trattare i dati personali soltanto su istruzione documentata del titolare del trattamento;
- garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza. 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;
- adottare tutte le misure adeguate di sicurezza ai sensi dell'art. 32 GDPR;
- non ricorrere ad altro Responsabile senza previa autorizzazione scritta del Titolare del trattamento;
- assistere il Titolare nel garantire il rispetto degli obblighi previsti dalla vigente normativa privacy, nazionale ed europea;
- cancellare o restituire al Titolare tutti i dati personali al termine della prestazione;
- mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare conformità agli obblighi previsti dalla vigente normativa privacy, nazionale ed europea;
- avvisare tempestivamente il Titolare del trattamento di un'eventuale violazione.

## **Art. 6**

### **Sub-Responsabile del Trattamento dei Dati Personali**

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;

Qualora un Responsabile del trattamento designato ricorra a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento. L'altro

Responsabile dovrà presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento.

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.

#### **Art. 7**

#### **Persona Autorizzata al Trattamento (PAT)**

La **Persona Autorizzata al Trattamento** seppur non specificamente prevista dal Regolamento è il soggetto, persona fisica, interno all'organizzazione del Titolare (dipendente, collaboratore, lavoratore atipico, etc.) che materialmente compie operazioni di trattamento sui dati personali, riconducibile pertanto alla figura dell'incaricato prevista dalla normativa nazionale precedente. La designazione non è attributiva di *status* in quanto il soggetto in questione è incaricato *ipso facto*, essendo il trattamento di dati personali inscindibilmente connesso alle mansioni svolte. Il Titolare, o chi per suo conto, ha l'obbligo di formare le PAT e di impartire loro le opportune istruzioni operative, cui attenersi nell'esecuzione delle attività di trattamento.

#### **Art. 8**

#### **Amministratore Di Sistema (ADS)**

Si tratta di una figura professionale essenziale per la sicurezza delle banche dati e la corretta gestione delle reti telematiche; è un esperto chiamato a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali; a lui viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informativi aziendali o di una pubblica amministrazione. L'amministratore di sistema può essere un soggetto **interno** (incaricato/soggetto designato) o **esterno** (responsabile esterno se trattasi di persona fisica; incaricato del responsabile esterno se il fornitore è una persona giuridica).

#### **Art.9**

#### **Finalità del trattamento**

1. I trattamenti sono compiuti dal Comune per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. 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 finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

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

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

## **Art. 10**

### **Diritti degli interessati**

Ai sensi degli artt. da 15 a 22 del Reg. UE 679/2018, i soggetti interessati, cui si riferiscono i dati, hanno il diritto:

- di essere informati sull'esistenza o no dei dati che lo riguardano;
- di averne comunicazione in forma comprensibile;
- di conoscere finalità e modalità di trattamento;
- di essere informati sulla logica applicata al trattamento, ivi compreso l'utilizzo di strumenti elettronici e di particolari forma di elaborazione.

### **A. Modalità di esercizio dei diritti**

I diritti elencati agli articoli 15-22 del Reg. UE 679/2016 sono esercitati dall'interessato con richiesta rivolta senza al Titolare o al Responsabile, anche per il tramite di un incaricato al quale è fornito idoneo riscontro senza ritardo.

L'interessato può conferire delega o procura a persone fisiche, enti, associazioni o organismi o farsi assistere da persona di fiducia.

L'identità dell'interessato è verificata mediante esibizione di un documento di riconoscimento.

La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato.

Ai sensi dell'art. 2 *terdecies* del D.lgs. n. 101/2018, i diritti di cui agli articoli 15-22 del GDPR riferiti ai dati personali di persone decedute, possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di protezione. Ciò non è ammesso nei casi previsti dalla Legge.

L'Ente indica all'interno di ciascuna informativa *privacy*, i contatti e gli eventuali altri recapiti (indirizzo, e-mail, ecc.), compresi i dati di contatto del DPO, mediante cui gli interessati possono esercitare i propri diritti.

In particolare, relativamente alle modalità di esercizio di tali diritti, il Titolare:

- è tenuto ad evadere la richiesta dell'interessato, verificata l'identità di detto soggetto;
- può richiedere ulteriori informazioni che attestino l'identità dell'interessato, qualora nutra ragionevoli dubbi a riguardo;
- ove la richiesta fosse incompleta, o su domanda dell'interessato, mette a disposizione di quest'ultimo i moduli per l'esercizio dei propri diritti di cui agli allegati di seguito riportati;
- deve fornire all'interessato, se tecnicamente possibile, le informazioni relative all'azione intrapresa riguardante una richiesta di cui agli artt. 15-22, laddove esercitabili, senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta stessa;
- può prorogare di due mesi il termine di evasione della richiesta, illustrando all'interessato le motivazioni di tale proroga;
- qualora non ottemperi alla richiesta dell'interessato, è tenuto ad informarlo dei motivi dell'inottemperanza e della possibilità di proporre reclamo ad un'autorità di controllo e ricorso giurisdizionale.

Le comunicazioni e le azioni intraprese ai sensi degli artt. 15-22 e dell'art. 34 del GDPR sono gratuite. Tuttavia, dimostrato il carattere manifestatamente infondato o eccessivo della richiesta dell'interessato, il Titolare può:

- addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire informazioni e comunicazioni o intraprendere l'azione richiesta;

-rifiutare di soddisfare la richiesta dell'interessato.

## **B. Conservazione**

In osservanza alle prescrizioni del quadro normativo vigente in materia di protezione dei dati personali, l'Ente individua, all'interno dell'informativa resa agli interessati, il periodo esatto di conservazione dei dati, ovvero i criteri cui ricorre per la determinazione di detto periodo. Nell'ottica di ottemperanza del principio di limitazione della conservazione dei dati personali trattati, si suggerisce di prevedere l'inserimento di un paragrafo dedicato a tale aspetto. Generalmente, l'individuazione dei tempi di conservazione avviene:

- ✓ in base alle finalità di trattamento dei dati personali, pertanto, per un arco temporale non superiore all'oro conseguimento;
- ✓ in base alle disposizioni di Legge;
- ✓ in base ad una determinazione del Titolare del trattamento.

Inoltre, l'Ente documenta il lasso temporale entro cui i dati vengono conservati e le modalità di conservazione degli stessi anche all'interno del registro.

L'Ente prevede, altresì, la cancellazione sicura e la rimozione permanente dei dati personali:

- decaduto il termine di conservazione;
- per assolvere alla eventuale richiesta di cancellazione avanzata dall'interessato ai sensi dell'art. 17 del GDPR (UE).

## **Art. 11**

### **Responsabile della protezione dati**

1. Il Responsabile della protezione dei dati è individuato in una figura unica alle dipendenze del Comune *ovvero professionista scelto tramite procedura ad evidenza pubblica*

Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile 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 sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (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 RGPD;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) altri compiti e funzioni a condizione che il Titolare o il Designato 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 il Designato 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 Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti 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 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 (*in relazione alle dimensioni organizzative del Comune*):

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

6. Il Titolare ed il Soggetto Designato 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, ovvero tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo 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 e dal Soggetto Designato del trattamento per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - od al Soggetto Designato del trattamento.

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

## **Art.12**

### **Sicurezza del trattamento**

1. Ciascun Responsabile del trattamento garantisce misure tecniche ed organizzative adeguate per 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 ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Soggetto Designato al 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.

4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. Ciascun Soggetto Designato al trattamento impartisce adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare, o dei Soggetti Designati al trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

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

### **Art. 13**

#### **Registro delle attività di trattamento**

1. Ai sensi dell'art. 30 GDPR ciascun/ciascuna Dirigente/Responsabile, designato/a con decreto del/della Sindaco/a ai sensi dell'art. 2-*quaterdecies* D.lgs. 196/2003, è responsabile della corretta tenuta del Registro delle attività di trattamento svolte per conto del Titolare nel proprio Settore di afferenza. Ciascun Registro reca le seguenti informazioni in ordine a tutti i trattamenti censiti dagli uffici del proprio Settore:

a) il nominativo ed i dati di contatto del Titolare del trattamento ovvero del Soggetto Designato nonché del DPO;

b) la base giuridica che rende lecito il trattamento;

c) le finalità del trattamento;

d) la descrizione delle categorie di interessati, nonché delle categorie di dati personali;

e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi gli eventuali destinatari di paesi terzi extra UE od organizzazioni internazionali;

f) l'eventuale presenza di un Responsabile del trattamento nominato ai sensi dell'art. 28 GDPR;

g) l'eventuale presenza di uno o più altri Titolari del trattamento, nel caso di trattamenti

effettuati in regime di contitolarità ai sensi dell'art. 26 GDPR;

h) il termine previsto per la cancellazione dei dati personali;

i) la descrizione delle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 9 del presente Regolamento.

2. Il Registro è tenuto in forma cartacea e/o digitale da ciascun Soggetto Designato ed è accessibile, dai soggetti della struttura organizzativa di afferenza opportunamente autorizzati, ai fini della registrazione di nuovi trattamenti o per l'aggiornamento dei trattamenti già censiti.

3. L'insieme aggregato dei Registri di Settore tenuti da ciascun Soggetto Designato costituisce, ai sensi dell'art. 30 GDPR, il Registro delle attività di trattamento del Titolare del trattamento.

## **Art. 14**

### **Obbligo di informativa**

1. In relazione a ciascun ambito di attività dell'Ente per cui sia prevista la raccolta di dati personali vi è obbligo in capo al Titolare di rendere l'informativa agli interessati che abbiano fornito direttamente i propri dati personali o per i quali i dati personali siano stati ottenuti indirettamente. Ciascun Soggetto Designato è tenuto a sovrintendere alla corretta redazione e somministrazione delle informative riferibili per materia ai propri uffici.

2. L'informativa deve essere allegata o richiamata dalla modulistica predisposta per il conferimento dei dati personali. Nel caso in cui la raccolta avvenga con altri mezzi, l'informativa deve essere comunque fornita all'interessato contestualmente all'atto stesso della raccolta dei dati. Qualora i dati non siano raccolti direttamente presso gli interessati, il Soggetto Designato provvede a somministrare l'informativa agli interessati nei modi e nei termini di cui all'art. 14 GDPR.

3. L'informativa può essere somministrata con modalità alternative e/o informatizzate, a condizione che ciò avvenga in conformità con il GDPR e le "Linee guida EDPB sulla trasparenza ai sensi del Regolamento 2016/679" adottate il 29 novembre 2017 ed emendate l'11 aprile 2018.

4. Ciascuna informativa, oltre ad essere chiara e concisa, deve contenere alcune informazioni essenziali che devono essere sempre comunicate o rese facilmente disponibili agli interessati, quali:

a) i dati di contatto del Titolare, con riferimento al Settore competente al trattamento;

b) i dati di contatto del DPO;

c) le finalità del trattamento cui sono destinati i dati personali raccolti;

d) la base giuridica che legittima il trattamento;

e) le categorie di destinatari dei dati personali, ivi compresi gli Uffici adibiti al trattamento medesimo, se individuabili;

f) il periodo di conservazione dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

5. Gli ulteriori contenuti della informativa, a seconda che i dati siano stati ottenuti o meno direttamente dagli interessati, sono disciplinati rispettivamente dagli artt. 13 e 14 GDPR.

## **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 Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.

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, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;

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; combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

f) 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;

g) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

h) 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.

- 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.

6. 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;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

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

7. Il Titolare 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.

8. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per

trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

9. 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.

11. E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

## **Art. 16**

### **Violazione dei dati personali**

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

2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. 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.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifrazione 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 RGPD, 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 Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

## **Art.17**

### **Rinvio**

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





