COMUNE DI LEI

REGOLAMENTO COMUNALE

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

SOMMARIO

GLOSSARIO

Regolamento (anche GDPR)

Il Regolamento U.E. 679/2016 e ss.mm.ii. "Regolamento Generale sulla Protezione dei dati" relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati".

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.

Interessato

Secondo la definizione di cui all'art. 4.1 del GDPR è interessato "la persona fisica identificata o identificabile" attraverso il trattamento dei dati personali oggetto del trattamento dei dati personali che la riguardano.

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.

Limitazione di trattamento:

Secondo la definizione di cui all'art. 4.3 del GDPR dicesi limitazione di trattamento "Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro";

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.

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;

Responsabile della protezione dei dati (di seguito, RPD o DPO)

Il soggetto, designato dal Titolare e dal Responsabile, incaricato di fornire consulenza e assistenza per l'esatta osservanza del RGPD ai sensi dell'art. 39 del GDPR;

Destinatario

La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Violazione dei dati personali

La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Misure tecniche e organizzative

- Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
- Sistemi di autenticazione, sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.
- Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico-adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.

  Ogni altra misura tecnica e organizzativa adeguata (tenuto conto, dei tempi, natura, costi, tecnologia) a far fronte e contrastare minacce alla integrità, disponibilità, riservatezza e resilienza del sistema di gestione del trattamento dei dati dell'Ente

CAPO I – OGGETTO E PRINCIPI

1. Il Regolamento UE 2016/679, ha introdotto nel nostro ordinamento giuridico il "*principio di accountability"* (responsabilizzazione), che impone alle Pubbliche Amministrazioni titolari del trattamento dei dati:

- ✓ di dimostrare di avere adottato le misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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;
- ✓ che i trattamenti siano conformi ai principi e alle disposizioni del Regolamento, prevedendo, altresì, l'obbligo del titolare della tenuta di apposito registro delle attività di trattamento, compresa la descrizione circa l'efficacia delle misure di sicurezza adottate;
- ✓ che il registro di cui al punto precedente, da tenersi in forma scritta o anche in formato elettronico deve contenere una descrizione generale delle misure di sicurezza tecniche e organizzative e che su richiesta, il titolare del trattamento è tenuto a mettere il registro a disposizione dell'autorità di controllo.

2. La nuova normativa europea impone quindi alle Pubbliche Amministrazioni di non limitarsi alla semplice osservanza di un mero adempimento formale in materia di privacy, conservazione e sicurezza dei dati personali, ma attua un profondo mutamento culturale con un rilevante impatto organizzativo da parte dell'Ente nell'ottica di adeguare le norme di protezione dei dati ai cambiamenti determinati dalla continua evoluzione delle tecnologie (quali ad esempio la interconnessione di banche dati e la pubblicazione automatizzata di dati on line) nelle amministrazioni pubbliche.

3. Il presente Regolamento ha per oggetto misure procedimentali 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 Lei.

Art. 1 Principi generali in materia di privacy

1. Il Comune di Lei, in qualità di Titolare del trattamento, garantisce l'applicazione dei principi fondamentali della privacy, sanciti dal GDPR ed identificati nella seguente tabella:

PRINCIPIO GENERALE E RIF. LEGGE DESCRIZIONE	DESCRIZIONE
LICEITÀ, CORRETTEZZA E TRASPARENZA (GDPR, Art. 6; Art.5, par.1, a)	1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. I dati sono trattati in modo corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
FINALITÀ' (GDPR, Art.5, par.1, b)	I dati personali sono raccolti e trattati solo per finalità predeterminate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
NECESSITÀ', NON ECCEDENZA, ESSENZIALITÀ (GDPR, Art.5, par.1, c)	I dati sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati). L'utilizzo dei dati personali è sempre ridotto al minimo necessario essenziale per il raggiungimento delle finalità dichiarate; i dati personali sono raccolti e trattati solo se funzionali al raggiungimento delle finalità dichiarate; i dati personali sono trattati con modalità e strumenti proporzionali alle finalità da raggiungere.
ESATTEZZA, COMPLETEZZA, AGGIORNAMENTO (GDPR, Art.5, par.1, d)	I dati personali sono puntualmente verificati, in modo che sia garantita la loro esattezza, completezza ed aggiornamento.
CONSERVAZIONE (GDPR, Art.5, par.1, e)	I dati personali sono conservati per un periodo di tempo al raggiungimento delle finalità dichiarate; i dati personali possono essere conservati per periodi più lunghi a condizione che siano

	trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal regolamento a tutela dei diritti e delle libertà dell'interessato (limitazione della conservazione);
SICUREZZA (GDPR, Art.5, par.1, f)	I dati sono sempre raccolti e trattati previa adozione di idonee misure di sicurezza, ovvero misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).
RISERVATEZZA (GDPR, Art.5, par.1, f)	I dati sono trattati da soggetti adeguatamente identificati.

CAPO II

Art. 2 Ruoli, compiti e nomina dei soggetti

1. Il Titolare del trattamento ha individuato figure interne alla struttura, che presidieranno i processi organizzativi atti a garantire un corretto trattamento dei dati personali, nonché la figura del Responsabile della Protezione dei dati personali (DPO/RPD), che operando in sinergia con il Titolare del trattamento e con gli altri soggetti interni alla struttura del Titolare, garantirà l'adozione di nuove misure tecniche ed organizzative volte a garantire l'integrità e la riservatezza dei dati, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la verifica e la valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza nel trattamento dei dati personali.

2.1 Il Titolare del Trattamento dei dati

1. Il Titolare del trattamento dei dati è il **Comune di Lei**, il quale provvede al trattamento dei dati personali tramite le proprie articolazioni organizzative e per lo svolgimento delle relative funzioni istituzionali (di seguito indicato con *"Titolare").*

2. Il Titolare, tramite le proprie articolazioni organizzative-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 tramite le proprie articolazioni organizzative mette in atto misure tecniche ed organizzative adeguate a garantire e 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.

4. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa di ciascuna articolazione organizzativa, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

5. Il Titolare tramite le proprie articolazioni organizzative adotta misure appropriate per fornire all'interessato:

- le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
- le informazioni indicate all'art. 14 RGPD, qualora i dati personali non siano 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- tramite le proprie articolazioni organizzative di volta in volta competenti per Area -una valutazione d'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP.

6. Il Titolare, per mezzo del presente regolamento, provvede a:

a) designare, nell'ambito delle Aree di cui al Regolamento degli Uffici e dei Servizi, i soggetti Designati al trattamento dei dati personali per l'esercizio delle funzioni e dei compiti indicati al successivo punto, ciascuno nella rispettiva Area di competenza e per la propria funzione di coordinamento/esecutiva, quali:

- il Responsabile dell'area Amministrativa, AA-GG, Sociale;
- il Responsabile dell'area Tecnica;
- il Responsabile dell'Area Finanziario-Tributi;
- il Segretario Comunale

Tali soggetti a propria volta provvederanno a individuare nell'ambito della propria area organizzativa i soggetti autorizzati al trattamento dei dati, fornendogli le specifiche istruzioni ai sensi e per gli effetti di cui all'art. 29 del GDPR come meglio dettagliato al successivo art. 2.2.3

b) nominare il Responsabile della protezione dei dati.

c) nominare -tramite le proprie articolazioni organizzative/soggetti designati di cui sopra- quale Responsabile del trattamento i soggetti pubblici o privati esterni all'organizzazione dell'Ente, 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 (in relazione alle dimensioni organizzative del Comune).

d) predisporre tramite le proprie articolazioni organizzative/soggetti designati di cui sopra l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente 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 e di mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. In tali ipotesi tramite le proprie articolazioni organizzative/soggetti designati di cui sopra, il Titolare predispone l'accordo che 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 del trattamento.
9. Il Titolare forma periodicamente tutti i soggetti che fanno parte dell'organizzazione, in modo da rendere effettiva e omogenea l'applicazione del GDPR nell'ambito dell'Ente

2.2- Soggetti Designati al Trattamento dei Dati

1. I soggetti Designati al trattamento dei dati assicurano il rispetto del Regolamento UE 2016/679 e dalla normativa nazionale in relazione agli obblighi a loro delegati dal Titolare del trattamento.
Fatta eccezione per le designazioni contenute nel presente atto rispetto ai propri obblighi legali previsti dal particolare ruolo dirigenziale e funzione apicale, tutti gli altri soggetti designati sono nominati mediante apposita nomina nella 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 nell'ambito dei Servizi cui sono preposti
- ✓ le istruzioni specifiche sul trattamento dei dati.

2. I Designati, in funzione delle proprie specifiche mansioni e del ruolo ricoperto, sono tenuti a porre in essere, nell'ambito della propria Area di appartenenza e nel rispetto delle proprie competenze, misure tecniche ed organizzative adeguate a garantire e dimostrare che il trattamento dei dati personali è effettuato conformemente alle disposizioni del predetto Regolamento.
3. Ai Designati sono altresì delegati i seguenti specifici compiti e funzioni:

a) nell'ambito dell'Area al quale sono preposti, designare il personale autorizzato al trattamento dei dati personali fornendo loro adeguate istruzioni per il corretto trattamento di detti dati, oltre a consentire idonea formazione in materia di trattamento dei dati personali del personale assegnato all'Area di rispettiva competenza ed a vigilare sulla corretta applicazione della normativa in materia da parte del medesimo personale
b) stipulare i contratti di cui all'art. 28, paragrafo 3, GDPR, per disciplinare il rapporto con il responsabile del trattamento e dargli le necessarie istruzioni
c) in caso di *data breach* dare immediata comunicazione al Sindaco nonché al DPO che coinvolgerà gli atri soggetti previsti dalla specifica procedura di gestione della Data Breach.
d) effettuare l'analisi del rischio e la valutazione dell'impatto di cui all'art. 35 Reg. UE 2016/679, nella funzione organizzativa di Sua competenza
e) adottare misure appropriate al fine di garantire l'esercizio dei diritti di coloro i cui dati personali sono oggetto di trattamento previsti agli articoli da 15 a 18 e da 20 a 22 del Regolamento;
f) verificare la corretta predisposizione delle informative e curarne il costante aggiornamento.

2.3- Persone autorizzate al trattamento con funzioni operative

1.I Designati/Responsabili del servizio di cui ai punti che precedono, individuano all'interno della propria struttura operativa, il personale dipendente autorizzato all'espletamento di tutte le operazioni relative al trattamento dei dati.
2. La designazione viene fatta con un atto scritto nel quale vengono specificati i compiti affidati alle persone autorizzate e le prescrizioni per un corretto, lecito, sicuro e pertinente trattamento dei dati medesimi.

3**.** Il personale in servizio presso il Comune di Lei che tratta dati personali in relazione alle competenze dell'Area al quale è stato assegnato, è autorizzato a trattare dati personali in relazione alle competenze attribuite, o comunque esercitate presso gli uffici a cui sono preposti e, comunque, nel rispetto delle misure e delle istruzioni adottate dai soggetti Designati/Responsabili del servizio.
4. Gli autorizzati effettuano tutte le operazioni di trattamento dei dati nel rispetto delle istruzioni impartite dal Soggetto Designato/Responsabile del servizio a cui fanno capo le quali prevedono:
-di accedere a quei dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti affidati;
-di trattare i dati personali di cui si viene a conoscenza per l'assolvimento dei propri compiti in modo lecito e corretto, nel rispetto della normativa vigente in materia e dei Regolamenti adottati dall'Ente;
- verificare continuamente i dati, i relativi aggiornamenti, la completezza e pertinenza dei medesimi, collaborando nella mappatura dei trattamenti e nella implementazione dei Registri tenuti dal Titolare;
- custodire con diligenza atti e documenti contenenti dati personali ricevuti al fine di adempiere ai compiti assegnati e restituirli una volta che sia espletato il compito assegnato;
-comunicare i dati personali trattati solo previa autorizzazione;
-osservare scrupolosamente e diligentemente le misure di sicurezza predisposte;
- osservare anche in seguito alla modifica e/o trasferimento o cessazione del rapporto di lavoro tutti gli obblighi in materia di riservatezza.
- ogni altra istruzione venga impartita nell'apposito atto di designazione

2.4- Attività di coordinamento e Gruppo di Lavoro

1. I soggetti Designati/Responsabili del servizio di cui al punto 2.1.6 fanno parte di diritto del Gruppo di lavoro sulla tutela dei dati personali che una volta costituito, potrà essere integrato con altri componenti opportunamente nominati.
Al gruppo di lavoro sono affidati i seguenti compiti:

- ✓ Definire e aggiornare i modelli di informativa da adottare;
- ✓ Coordinare l'aggiornamento del Registro delle attività di trattamento;
- ✓ Definire le procedure di gestione degli eventi che comportano una violazione dei dati personali (*data breach*), di notifica delle violazioni all'autorità di controllo e la comunicazione all'interessato;
- ✓ Definire criteri comuni per le modalità di esercizio dei diritti adottare misure appropriate al fine di garantire l'esercizio dei diritti di coloro i cui dati personali sono oggetto di trattamento previsti agli articoli da 15 a 18 e da 20 a 22 del Regolamento UE 2016/679;
- ✓ Discutere e valutare ogni problematica relativa alla tutela dei dati personali;
- ✓ Proporre l'adozione di procedure, regolamenti e provvedimenti migliorativi delle pratiche di trattamento, di gestione e di tutela dei dati personali.

2. Il Segretario Comunale svolge le funzioni di coordinamento del Gruppo di lavoro, fornendo indicazioni di carattere generale alle diverse Aree dell'Ente in termini di definizione delle politiche in materia di trattamento dei dati personali.

2.5- Responsabile del trattamento dei dati

1. La funzione di Responsabile del trattamento discende da contratto, sottoscritto dal Titolare del trattamento, oppure sottoscritto dai soggetti Designati/Responsabili del servizio.

2. Il Responsabile del servizio nomina quali Responsabili del trattamento i soggetti pubblici o privati affidatari, per conto del Comune, di attività e servizi che per la loro corretta realizzazione rendono necessario il trattamento dei dati medesimi o soggetti terzi che trattano i dati sulla base di specifiche convenzioni.
3. Il Responsabile del servizio impartisce adeguate istruzioni relative al trattamento dei dati nel contratto di affidamento o con atto separato nel quale vengono definiti la materia, natura e finalità del trattamento medesimo, il tipo di dati che verranno trattati, le categorie di soggetti interessati dal trattamento oltre agli obblighi che incombono sul responsabile e che il medesimo si vincola a rispettare con la sottoscrizione dei suddetti atti.
4. I responsabili del trattamento sono nominati tra soggetti che offrono le garanzie elencate nell'art. 28, par. 1 del GDPR e tale sussistenza deve essere oggetto di espressa dichiarazione e deve espressamente accettare di sottoporsi ad Audit e controlli periodici.
5. Il Responsabile del trattamento tratta i dati personali in applicazione di quanto espressamente previsto nel contratto stipulato tra le parti ed ai sensi degli articoli 28, 29, 30 e 31 del Regolamento Europeo 2016/679, in ordine a:

- ✓ materia disciplinata e durata del trattamento;
- ✓ natura e le finalità del trattamento;
- ✓ tipo di dati personali;
- ✓ categorie di interessati;
- ✓ obblighi e i diritti del Titolare del trattamento.

6. Gli atti che disciplinano il rapporto tra il Titolare del Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p.3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
7. È consentita la nomina, previa l'autorizzazione del Responsabile del servizio dell' Area interessata, 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.
8. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento.
9. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita ed idonea formazione ed istruzione e si sia impegnato alla riservatezza o abbia un adeguato obbligo legale di riservatezza.
10. 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 in maniera indicativa e non esaustiva provvede:

- ✓ alla tenuta del registro delle categorie di attività di trattamento svolto per conto del Titolare;
- ✓ all'adozione di idonee misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti;
- ✓ alla sensibilizzazione e dalla formazione del personale che partecipa ai trattamenti e dalle connesse attività di controllo;
- ✓ alla designazione *(qualora sia obbligato)* del Responsabile per la Protezione dei Dati (RPD);

- ✓ 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.

2.6- Responsabile della Protezione dati - DPO

1. Il Responsabile della Protezione dei Dati assolve ai compiti previsti dall'art. 39 del Regolamento UE 2016/679 e gli eventuali altri compiti affidati.

2. Il Responsabile della protezione dei dati viene individuato con un decreto di nomina da parte del Sindaco che stabilisce la durata dell'incarico.

3. Il Comune sostiene il Responsabile Protezione Dati nell'esecuzione dei compiti ad esso affidati assicurando l'autonomia e le risorse necessarie per assolverli come previsto dall'art. 38 del Regolamento UE 2016/679.

4. Il RPD è incaricato dei seguenti compiti:

- ✓ informare e fornire consulenza al Titolare 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.
- ✓ sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare 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 ai seguenti aspetti: 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 salvaguardi e applicare) siano conformi al RGPD;
- ✓ 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 al Garante;

5. Il Titolare del trattamento tramite le proprie articolazioni organizzative/soggetti designati assicura 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 soggetti Designati 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 RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati.

6. I Responsabili del servizio/Designati consultano il DPO in ordine alle attività di adeguamento dell'Ente alla normativa in materia di protezione dei dati personali dando priorità a quelle attività che presentino maggiori rischi inerenti la protezione dei dati. Il DPO assiste il Titolare evidenziando le priorità di intervento,

7. Gli uffici formulano le proprie richieste al RPD il quale trasmette i risultati della propria attività consultiva di norma entro 30 giorni dalla richiesta.

2.7- Amministratore di sistema

1. L'amministratore di sistema sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione.

2. L'amministratore di sistema svolge attività quali il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.

3. Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (*access log*) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

4. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.

5. L'amministratore di sistema è destinatario degli interventi di formazione di aggiornamento, qualora si tratti di soggetto appartenente all'Organizzazione del Titolare.

6. Gli specifici compiti e le responsabilità dell'AdS sono regolati da specifico atto di designazione del Titolare

CAPO III- ATTIVITÀ DI TRATTAMENTO DATI PERSONALI

Art. 3.1 Liceità del trattamento

1. Il trattamento dei dati personali deve essere svolto in modo lecito, corretto e trasparente, secondo quanto previsto dall'art. 5 del GDPR.

2. La raccolta dei dati deve avvenire per finalità determinate, esplicite e legittime e i dati possono essere trattati in modo che l'attività da svolgere non sia incompatibile con tali finalità.

3. All'interessato o alla persona che fornisce i dati, al momento della raccolta degli stessi, deve essere fornita una idonea informativa, secondo quanto previsto e nelle forme di cui agli articoli 13 e 14 del GDPR.

4. Oltre, all'obbligo di informativa, affinché il trattamento dei dati sia lecito, occorre che siano rispettate le regole previste rispettivamente per la raccolta ed il trattamento dei dati comuni e dei dati particolari dagli articoli 6 e 9 del GDPR.

Art. 3.2 Finalità del trattamento e base giuridica del trattamento

1. Il Titolare garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.

2. Il Titolare, nell'ambito delle sue funzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi, inclusi i procedimenti amministrativi di competenza del Titolare, vanno gestiti conformemente alle disposizioni del Codice, del GDPR, e del presente Regolamento. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina.

3. In conformità a quanto sancito dall'art. 6 dal GDPR il trattamento è lecito solo se e nella misura in cui ricorra almeno una delle seguenti condizioni:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento. Solo a titolo esemplificativo rientrano in questo ambito i seguenti trattamenti:

- ✓ accesso a documenti amministrativi e accesso civico;
- ✓ tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia;
- ✓ tenuta di registri pubblici relativi a beni immobili o mobili;
- ✓ cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
- ✓ elettorato attivo e passivo ed esercizio di altri diritti politici;
- ✓ esercizio del mandato degli organi rappresentativi;
- ✓ svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo;
- ✓ attività di controllo e ispettive;
- ✓ concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- ✓ conferimento di onorificenze e ricompense;
- ✓ rapporti tra i soggetti pubblici e gli enti del terzo settore;
- ✓ obiezione di coscienza;
- ✓ attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- ✓ compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario;
- ✓ istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- ✓ instaurazione, gestione ed estinzione, di rapporti di lavoro.
- ✓ l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

b) l'adempimento di un obbligo legale al quale è soggetto il Comune.

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

d) il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

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

Art. 3.3 Condizioni per il consenso

1. Il Comune, in quanto soggetto pubblico, non deve richiedere il consenso all'interessato in merito al trattamento dei dati personali, purché il trattamento sia conforme al perseguimento di fini istituzionali dell'Ente ai sensi dell'art. 3.2 del presente regolamento.

2. Nelle limitate ipotesi in cui il consenso debba essere richiesto questo deve essere libero, informato e espresso in modo inequivocabile, con tutte le caratteristiche indicate nella normativa vigente.

3. Difatti, qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

4. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

5. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prestato prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

6. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

7. Per i dati sensibili il consenso deve essere esplicito e in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione.

8. Il consenso deve essere, in tutti i casi, libero e autonomo, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto.

7. Il consenso deve essere manifestato attraverso dichiarazione o azione positiva inequivocabile.

9. La manifestazione del consenso, ad opera dell'interessato, va resa al momento del primo accesso alle prestazioni, ed è valido ed efficace fino alla revoca della stessa o, per i minorenni, fino al compimento del diciottesimo anno di età.

10. Il consenso viene registrato nel registro delle attività di trattamento.

Art. 3.4 Informativa

1. L'interessato deve essere preventivamente informato, , secondo quanto previsto dagli artt. 13 e 14 del GDPR.

2. L'informativa deve essere facilmente intellegibile per l'interessato, accessibile, concisa e improntata alla trasparenza. Occorre utilizzare un linguaggio semplice e chiaro.

3. Nell'informativa devono essere comunicati altresì i dati del soggetto che effettua il trattamento.

4. Ciascun Responsabile del servizio, con il supporto del DPO e previa valutazione delle modifiche vagliate dal medesimo DPO, è tenuto a tenere sempre aggiornate le informative utilizzate.

5. L'informativa può essere resa disponibile dagli uffici o mediante pubblicazione nel sito istituzionale dell'Ente. Si deve dare prevalenza alla forma scritta in modo da documentare sempre di aver reso l'informativa agli interessati

CAPO IV - REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Art. 4.1 Registro delle attività di trattamento

1. In conformità a quanto sancito dall'art. 30 paragrafo 1 GDPR, 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 soggetto Designato, eventualmente del Contitolare del trattamento, del RPD;

b) le finalità e la base giuridica 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.

2. Il Registro è tenuto dal Titolare tramite le proprie articolazioni organizzative/soggetti designati, presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative e delle esigenze specifiche dell'Ente.

4. I soggetti Designati provvedono all'aggiornamento del registro delle attività di trattamento con riferimento agli ambiti di competenza e delle Aree a cui sono preposti.

- ***Art. 4.2 Registro delle categorie di attività trattate per conto di altri Titolari (art. 30 paragrafo 2 GDPR)***

1. Il Registro delle categorie di attività trattate da ciascun Designato reca le seguenti informazioni:

a) il nome ed i dati di contatto del Designato al trattamento e del RPD;

b) le categorie di trattamenti effettuati da ciascun Designato: 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.

2. Il Registro è tenuto dal Designato al trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea.

CAPO V

Art. 5 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 per il tramite le proprie articolazioni organizzative/soggetti designati secondo l'Area di competenza, 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 di mostrare 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:

- ✓ 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;
- ✓ 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 suddette persone fisiche;
- ✓ 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;
- ✓ trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
- ✓ 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;
- ✓ 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;
- ✓ utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
- ✓ trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01;
- ✓ trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

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 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.

5. I soggetti Designati devono assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. L'Amministratore di Sistema, se nominato, e/o l'ufficio competente perdetti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

6. 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.

7. 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.

8. 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.

9. 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 e dalla 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. 6 VIOLAZIONE DEI DATI PERSONALI

Art. 6.1

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 autorizzato l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune di Lei.

2. Chiunque venga a conoscenza di una violazione dei dati personali è tenuto a segnalarlo immediatamente, al proprio superiore gerarchico il quale provvede ad avvisare tempestivamente il Responsabile del servizio/Designato, il Segretario Comunale, il Sindaco, l'Ads e l'RPD/DPO

3. Il Titolare del trattamento tramite le proprie articolazioni organizzative/soggetti designati, ove necessario, notifica la violazione dei dati personali al Garante della Protezione dei Dati Personali entro 72 ore dal momento in cui ne sia venuto a conoscenza e comunque senza ingiustificato ritardo, a meno che sia improbabile che la stessa violazione presenti un rischio per la tutela dei diritti e delle libertà delle persone fisiche. La notifica viene effettuata, prevedendo almeno gli elementi indicati al paragrafo 3 dell'art. 33 del Regolamento Europeo 2016/679.

4. La notifica al Garante della protezione dei dati personali effettuata oltre le 72 ore, deve essere motivata.

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

- ✓ danni fisici, materiali o immateriali alle persone fisiche;
- ✓ perdita del controllo dei dati personali;
- ✓ limitazione dei diritti, discriminazione;
- ✓ furto o usurpazione d'identità;
- ✓ perdite finanziarie, danno economico o sociale.
- ✓ decifratura non autorizzata della pseudonimizzazione;
- ✓ pregiudizio alla reputazione;
- ✓ perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

6. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di far comprendere loro la natura della violazione dei dati personali verificatesi.

7. 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).

8. 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 *(registro data breach).* 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. 6.2 Comunicazione e diffusione di dati personali comuni

1.La comunicazione dei dati personali all'interno degli uffici dell'Ente per lo svolgimento delle funzioni istituzionali assegnate non è soggetta a limitazioni, fatte salve quelle previste da norme di legge e regolamento.

2.Il Titolare tramite le proprie articolazioni organizzative/soggetti designati competenti può adottare tutte le misure che ritiene opportune e necessarie al fine di tutelare il diritto alla riservatezza dei soggetti interessati.

3. È sempre vietata la diffusione/pubblicazione di dati personali particolari relativi alla salute.

ART. 7 RINVIO

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