Regolamento per il trattamento dei dati personali (Regolamento UE 2016/679)

Art. 1 - Oggetto

1. L'oggetto del presente Regolamento contiene disposizioni di attuazione del Regolamento UE (General Data Protection Regulation del 27 aprile 2016 n. 679, Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo al trattamenti dei dati personali, nonché alla libera circolazione di tali dati.
2. Le figure del sistema di protezione e trattamento dei dati personali sono il Titolare del trattamento, di cui all'art. 2 del Regolamento, il Responsabile del trattamento (art. 6 del Regolamento), il Subresponsabile del trattamento (art. 7) e il Responsabile della protezione dei dati, di cui all'art. 8 del presente Regolamento.
3. I nominativi e i dati di contatto del Titolare del trattamento, dei Responsabili e dei Subresponsabili del trattamento e del Responsabile della protezione dati sono resi noti mediante pubblicazione sul sito web istituzionale del Comune, sezione Amministrazione trasparente.

Art.2 - Titolare del trattamento

1. Il Comune, rappresentato ai fini previsti dal Regolamento UE 2016/679 dal Sindaco ai sensi dell'art. 50 comma 2 del d. lgs. n. 267/2000, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee.
2. Il Titolare del trattamento è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del Regolamento UE: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare del trattamento:
a) designa i Responsabili del trattamento nelle persone dei Responsabili di posizione organizzativa, al vertice delle strutture organizzative di massima dimensione in cui si articola l'organizzazione comunale. Tali Responsabili sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle aree organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati e può 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 tali soggetti esterni, 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;
b) nomina il Responsabile della protezione dei dati;
c) predispone l'elenco dei Responsabili del trattamento, da pubblicare in apposita sezione del sito istituzionale. L'elenco è soggetto ad aggiornamento periodico.

Art. 3 Misure di sicurezza

1. Il Titolare del trattamento pone in atto misure tecniche e organizzative adeguate per garantire che il trattamento di dati personali è effettuato in modo conforme al suddetto Regolamento UE 2016/679 e garantire la sicurezza nel trattamento dei dati, con le modalità indicate nell'art. 9 del presente Regolamento.
Le misure sono definite fin dalla fase di progettazione e poi della loro applivazione in maniera idonea a dare efficacia ai principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli artticoli da 15 a 22 del Regolamento UE, 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 del Documento unico di programmazione (DUP), del bilancio unico di previsione e del Piano esecutivo di gestione, previa analisi della situazione in essere, tenuto conto

dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e dei rischi dallo stesso derivanti, in relazione alla loro diverso grado di probabilità e gravità diverse in ordine ai diritti e le libertà delle persone fisiche.
2. Il Titolare adotta misure appropriate per fornire all'interessato:
a) le informazioni indicate dall'art. 13 del Regolamento UE, qualora i dati personali siano raccolti presso l'interessato;
b) le informazioni indicate dall'art. 14 del Regolamento UE, qualora i dati personali non stati ottenuti presso lo stesso interessato.
3. 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 procedere con una preventiva valutazione del suo impatto sulla protezione dei dati personali, come stabilito dall'art. 35 del Regolamento UE, tenendo conto della natura, oggetto, contesto e finalità del trattamento, tenuto conto di quanto indicato dal successivo art. 12.

Art. 4 – Funzioni e servizi svolti in forma associata

1. La condizione di contitolarità, prevista dall'art. 26 del Regolamento UE, si realizza 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. In tal caso, i distinti titolari del trattamento determinano congiuntamente le finalità ed i mezzi del trattamento mediante un accordo che definisce le responsabilità di ciascun soggetto coinvolto 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 Regolamento, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile. Nell'accordo può essere stabilito un punto di contatto comune per gli interessati.
2. Il Comune favorisce l'adesione a 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 Regolamento UE e per il suo concreto rispetto.

Art. 5 - 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 e 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.
b) l'adempimento di un obbligo di legge al quale è soggetto il Comune.
c) l'esecuzione di un contratto, nei confronti dei soggetti interessati;
d) specifiche finalità diverse da quelle descritte nei precedenti punti. In tali casi è necessario che l'interessato esprima il consenso al trattamento.
2. Le finalità del trattamento, nei casi previsti dalle lettere a) e b) del comma precedente sono stabilite dalle norme di legge che lo disciplinano.
3. 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. 6 - Responsabile del trattamento

1. I Responsabili di posizione organizzativa, titolari delle strutture organizzative di massima dimensione dell'Ente, sono nominati in qualità di Responsabile del trattamento dei dati relativi alle le banche dati esistenti nella struttura organizzativa di rispettiva competenza.
2. I Responsabili del trattamento sono designati mediante decreto del Sindaco, Titolare del trattamento, nel quale sono esplicitati tutti gli elementi previsti dall'art. 28 del Regolamento UE e, in particolare:
- la tipologia, la durata, la natura e la finalità del trattamento dei dati assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi e i diritti del Titolare del trattamento.
3. Il Titolare può avvalersi, per il trattamento dei dati di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 1, specificando nei relativi atti di conferimento dell'incarico 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.
4. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia stato idoneamente formato e istruito e osservi l'obbligo legale di riservatezza.
5. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
a) alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
b) all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
c) alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
d) ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati fornendo allo stesso ogni informazione di cui è in possesso;
e) ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica al Garante della 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. 7 – Sub responsabile del trattamento

1. Il Responsabile del trattamento può nominare uno o più sub-responsabili del trattamento per specifiche attività di trattamento, nel rispetto dei medesimi obblighi loro imposti dal Titolare del trattamento in virtù dell'atto di nomina.
2. I Sub responsabili del trattamento operano sotto la diretta autorità del Responsabile, attenendosi alle istruzioni impartite e nei limiti specifici dell'ambito del trattamento delegato dal Responsabile.
3. Il Responsabile del trattamento risponde dell'operato del sub-responsabile.

Art. 8 - Responsabile della protezione dati

1. Il Responsabile della protezione dei dati può essere individuato:
- in un dipendente dell'Ente, inquadrato nella cat. D con profilo professionale di Istruttore direttivo;
- in un soggetto esterno selezionato mediante procedura ad evidenza pubblica fra soggetti aventi le medesime qualità professionali richieste al dipendente, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili; i compiti attribuiti al RPD sono indicati in apposito contratto di servizi;
- in un soggetto unico, anche esterno alla pubblica amministrazione o alle pubbliche amministrazioni interessate, designato da più Enti locali mediante esercizio associato della funzione nelle forme previste dal D.Lgs. 18 agosto 2000 n. 267.
La figura di Responsabile è incompatibile con quelle che hanno fra i propri compiti la funzione di determinare le finalità o i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Responsabile del trattamento;
- ogni altro incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento

2. Il Responsabile della protezione dei dati svolge i 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 Regolamento UE e dalle altre fonti normative relative alla protezione dei dati. Il Responsabile della protezione dei dati può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) verificare la corretta osservanza del Regolamento UE 2016/679 e delle altre disposizioni normative relative alla protezione dei dati. In tale ambito, può procedere alla 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) monitorare le attribuzioni delle responsabilità delle varie figure coinvole nel trattamento dei dati e le attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire pareri sulla valutazione di impatto sulla protezione dei dati e monitorarne lo svolgimento.

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 del Regolamento UE.

f) può essergli conferito il compito di tenere il registro delle attività di trattamento e il registro delle categorie degli atti trattati di cui agli artt. 10 e 11 del Regolamento;

g) ulteriori compiti e funzioni nel campo del trattamento dei dati e della protezione della riservatezza, ad eccezione di quei ruoli o funzioni che possano condurre a un conflitto d'interesse, anche potenziale.

2. Il Titolare ed il Responsabile del trattamento assicurano che il Responsabile della protezione dei dati riceva tempestiva e adeguata informazione di ogni fattispecie riguardante la protezione dei dati personali. A tal fine:

- deve essere convocato alle riunioni di coordinamento dei Responsabili di posizione organizzativa che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- ricevuta l'informativa, emette parere sulle decisioni che impattano sulla protezione dei dati. Il parere ha carattere obbligatorio ma non è vincolante. Qualora la decisione assunta si discosti dalle indicazioni del Responsabile della protezione dei dati, deve contenere esplicita e sufficiente motivazione;
- deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro evento suscettibile di mettere a rischio la protezione dei dati.

3. Nello svolgimento dei compiti affidatigli il Responsabile della protezione dei dati individua e valuta i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso:

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

b) definisce un piano annuale di attività, in ordine di priorità nell'attività da svolgere, incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

5. Il Responsabile della protezione dei dati opera in posizione di autonomia e di terzietà rispetto alle altre figure del sistema di protezione dei dati e non può essere sollevato dall'incarico per questioni riguardanti l'adempimento dei suoi doveri, escluso il caso di negligenza e violazione di obblighi legislativi e regolamentari. Ferma restando l'indipendenza nello svolgimento di tali compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - od al Responsabile del trattamento.

6. Tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente:

- può disporre delle strutture organizzative e logistiche dell'Ente a supporto della sua attività;
- possono essergli assegnate risorse finanziarie, da gestire mediante la struttura organizzativa individuata per il supporto;

- può accedere a tutti i settori funzionali dell'Ente per acquisire informazioni necessarie alla propria attività e fornire supporto agli stessi nelle questioni relative al trattamento dei dati.

Art. 9 - Sicurezza del trattamento dei dati

1. Sono messe in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza del trattamento dei dati commisurato al rischio, tenendo conto dello stato di avanzamento delle soluzioni tecnologiche, dei costi di attuazione, della natura del contesto e del campo di applicazione, delle finalità del trattamento, del grado di probabilità del rischio e del livello di 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, in via non esaustiva:
a) la pseudonimizzazione (l'utilizzo di alias o di identità inesistenti), la minimizzazione (il trattamento dei soli dati effettivamente necessari) e la cifratura dei dati personali;
b) l'idoneità ad assicurare in continuum riservatezza, integrità e disponibilità dei sistemi di trattamento dei dati;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
d) la possibilità di disporre di una procedura di test per verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Costituiscono misure tecniche e organizzative, in via non esaustiva:
a) sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
b) misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi;
c) porte, armadi e contenitori dotati di serrature e ignifughi;
d) sistemi di copiatura e conservazione di archivi elettronici;
e) altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
4. Alle figure coinvolte nella gestione dei dati, Responsabili e Subresponsabili del trattamento sono impartite adeguate istruzioni sul rispetto delle predette.

Art. 10 - Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
a) i dati di contatto del Comune, Titolare del trattamento, il nominativo e i dati di contatto del Sindaco – legale rappresentante e del Responsabile della protezione dei dati;
b) le finalità del trattamento;
c) la descrizione sintetica delle categorie di interessati, nonché le categorie di dati personali oggetto di trattamento;
d) le categorie di soggetti a cui i dati personali sono stati o saranno comunicati;
e) l'eventuale trasferimento di dati personali verso un paese terzo o una organizzazione internazionale;
f) ove stabiliti, i termini per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, di cui agli artt. 3 e 9 che precedono.
2. Il Registro è tenuto dal Titolare del trattamento, eccdetto il caso in cui l'Ente si avvaglga della facoltà di affidarlo al Responsabile della protezione dei dati, di cui all'art. 8 comma 2 lett. f) del Regolamento, in tal caso, sempre sotto la responsabilità del Titolare del trattamento.
3. Il Titolare può stabilire di tenere un unico Registro dei trattamenti che contiene le informazioni di cui ai commi precedenti e quelle di cui al successivo art. 11, adottando la tipologia di registro, secondo lo schema allegato C al presente Regolamento. In tal caso, il Titolare delega la sua tenuta al Responsabile del trattamento, ovvero affida tale compito al Responsabile della protezione dei dati, come previsto dall'art. 8 comma 2 lett. f).

Art. 11 - Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Responsabile del trattamento reca le seguenti informazioni:
a) il nominativo e i dati di contatto del Responsabile del trattamento e del Responsabile per la protezione dei dati;
b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
c) l'eventuale trasferimento di dati personali verso un paese terzo o una organizzazione internazionale;
d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica, secondo lo schema allegato B al presente regolamento.
3. La tenuta del registro può essere affidata al Responsabile della protezione dei dati, ai sensi dell'art. 8 comma 2 lett. f), sempre comunque sotto la responsabilità del Responsabile del trattamento dei dati.

Art. 12 - Valutazioni d'impatto sulla protezione dei dati

1. Qualora il trattamento di dati, per la natura, l'oggetto, il contesto e le finalità, ovvero per l'impiego 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 preliminare dell'impatto del medesimo trattamento ai sensi dell'art. 35 del Regolamento UE 2016/679. La valutazione è una procedura che permette di verificare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la valutazione d'impatto sulla protezione dei dati, si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante della Privacy ai sensi dell'art. 35, paragrafi 4-6, del Regolamento UE.
3. In ogni caso, la valutazione d'impatto è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, paragrafo 3, del Regolamento UE, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ovvero trattamenti finalizzati ad assumere decisioni che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c) monitoraggio sistematico, ovvero 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 di natura estremamente personale, rientranti nelle categorie particolari di dati personali di cui all'art. 9 del Regolamento UE 2016/679;
e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento in termini numerici o di percentuale rispetto alla popolazione di riferimento, volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento, durata o persistenza dell'attività di trattamento, ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, ovvero dati riferiti a soggetti particolarmente vulnerabili e meritevoli di specifica tutela, per i quali si possa individuare una situazione di disequilibrio nel

rapporto con il Titolare del trattamento, come, ad esempio, i dipendenti dell'Ente, i soggetti con patologie psichiatriche, i richiedenti asilo, i soggetti anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, siano suscettibili di impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.
Nel caso in cui un trattamento presenti almeno due dei criteri sopra indicati occorre, in via generale, condurre una valutazione d'impatto sulla protezione dei dati, salvo motivata valutazione contraria del Titolare del trattamento, così come con motivata decisione, può essere sottoposto a valutazione d'impatto anche un trattamento che presenti soltanto uno dei criteri di cui sopra. La decisione di effettuare o non effettuare la valutazione è comunque sottoposta a parere preventivo del Responsabile per la protezione dei dati, che monitora e verifica lo svolgimento della valutazione e presta l'assistenza necessaria, insieme al Responsabile del trattamento e al responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi.
4. Il Titolare del trattamento garantisce l'effettuazione della valutazione d'impatto ed è responsabile della stessa, ma può affidare la conduzione materiale della valutazione ad altro soggetto, interno o esterno al Comune.
5. Il Responsabile della protezione dei dati può proporre lo svolgimento di una valutazione d'impatto in rapporto a uno specifico trattamento, proponendo la relativa metodologia per definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Tale facoltà è esercitabile anche dal responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, con riguardo alle esigenze di sicurezza o operative dei sistemi.
6. La valutazione d'impatto sulla protezione dei dati non è necessaria nei casi seguenti:
a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del Regolamento UE 2016/679;
b) se la natura, l'ambito, il contesto e le finalità del trattamento sono analoghe a quelli di un trattamento per il quale è già stata condotta una valutazione d'impatto. In tal caso si possono utilizzare i risultati della valutazione svolta per il trattamento similare;
c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima dell'ntrata in vigore del Regolamento UE 2016/679, in condizioni specifiche che non hanno subito modifiche;
d) se un trattamento trova il proprio legale fondamento nella legislazione in vigore che specificamente lo disciplina ed è stata già realizzata una valutazione d'impatto all'atto della definizione del fondamento giuridico anzidetto.
Inoltre, non è necessario condurre una valutazione d'impatto per quei trattamenti che siano già stati oggetto di verifica preliminare o di autorizzazione da parte del Garante della Privacy o di verifica preliminare del Responsabile della protezione dei dati e che proseguano con le stesse modalità che sono state oggetto di tale verifica.
7. La valutazione d'impatto sulla protezione dei dati è realizzata attraverso i seguenti processi:
a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e dell'eventuale esistenza di codici di condotta. 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:
1) delle finalità specifiche, esplicite e legittime;
2) della liceità del trattamento;
3) dei dati adeguati, pertinenti e limitati a quanto necessario;
4) del periodo limitato di conservazione;
5) delle informazioni fornite agli interessati;
6) del diritto di accesso e della portabilità dei dati;
7) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
8) dei rapporti con i responsabili del trattamento;
9) delle garanzie per i trasferimenti internazionali di dati;
10) consultazione preventiva del Garante della privacy;
c) valutazione dei rischi per i diritti e le libertà degli interessati, considerando 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 e attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento al Regolamento UE, tenuto conto dei diritti e degli interessi legittimi degli interessati e di tutti gli altri soggetti coinvolti.
8. Nell'ambito del procedimento di valutazione, possono essere consultati gli interessati. La mancata efettuazione della consultazione preventiva è specificatamente motivata, così come la decisione assunta in senso difforme dai risultati della consultazione degli interessati.
9. Qualora dalle risultanze della valutazione d'impatto sulla protezione dei dati indichinon l'esistenza di un rischio residuale elevato, corre l'obbligo del Titolare del trattamento di consultare il Garante della Privacy; tale necessità sussiste 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 ad esempio i trattamenti connessi alla protezione sociale e alla sanità pubblica.
10. La valutazione d'impatto deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso di dati 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. 13 - Violazione dei dati personali

1. Per violazione dei dati personali (definito "*data breach*" dal Regolamento UE 2016/679) si intende la violazione di sicurezza accidentale o illecita che comporta 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 del trattamento, 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 della Privacy entro 72 ore dall'evento e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare senza ritardo il Titolare, di violazioni dei dati personali, per la notifica al Garante.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del Regolamento UE 2016/679, 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).

5. Se il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, il Titolare del trattamento ne dà informazione agli interessati senza ritardo. I rischi per i diritti e le libertà degli interessati possono essere considerati elevati quando la violazione può, in via non esaustiva e meramente esemplificativa:
- coinvolgere un rilevante quantitativo di dati personali e/o numero 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);
- colpire soggetti che possono vulnerabili per le loro condizioni soggettive o oggettive (ad esempio utenti deboli, minori, disabili).

6. La notifica della violazione al Garante della privacy e l'informativa agli interessati devono essere conformi al contenuto minimo previsto dall'art. 33 del Regolamento UE e prevedere le informazioni e misure ivi previste.

7. 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 si intendono adottare per porvi rimedio devono essere adeguatamente documentate. La documentazione relativa alle violazioni deve essere conservata e fornita in caso di richiesta al Garante Privacy al fine di verificare il rispetto delle disposizioni del Regolamento UE 2016/679.

Art. 14 - 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.

Art. 15 – Entrata in vigore

1. Il Regolamento entrerà in vigore decorsi giorni quindici dalla pubblicazione all'albo pretorio, successiva alla intervenuta esecutività della deliberazione di approvazione.
2. A decorrere dall'entrata in vigore, sono abrogate le disposizioni regolamentari dell'Ente in materia di protezione della riservatezza, contrastanti con le nuove discipline.

ALLEGATI:

A) Registro delle attività di trattamento;

B) Registro delle categorie di attività di trattamento;

C) Registro unico dei trattamenti

A) Registro attività di trattamento

Frontespizio

REGISTRO ATTIVITA' DI TRATTAMENTO (art. 30, c.1, GPRD)

ENTE TITOLARE DEL TRATTAMENTO		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Registro tenuto da**	
Indirizzo		**Data di creazione**	
N. telefono		**Ultimo aggiornamento**	
Mail		**N. schede compilate**	
PEC		**Prossima revisione**	

Contenuto

	TRATTAMENTO			DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Contitolare (eventuale Rappres.nte)	Categoria	Dati sensibili (SI/NO)	Termine ultimo cancell.ne	Categoria	Consenso (SI/NO)	Categoria	Paesi terzi, org.ni int.li (eventuale) (SI/NO)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

B) Registro categorie di attività di trattamento

Frontespizio

REGISTRO CATEGORIE DI ATTIVITA' DI TRATTAMENTO (art. 30, c.2, GPRD)

ENTE TITOLARE DEL TRATTAMENTO		**Responsabile del trattamento**	

Contenuto

C) Registro unico dei trattamenti

Frontespizio

REGISTRO UNICO DEI TRATTAMENTI (art. 7, c.8, Regolamento comunale)			
ENTE TITOLARE DEL TRATTAMENTO		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Registro tenuto da**	
Indirizzo		**Data di creazione**	
N. telefono		**Ultimo aggiornamento**	
Mail		**N. schede compilate**	
PEC		**Prossima revisione**	

Contenuto

	TRATTAMENTO					DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Categorie	eventuale diverso Titolare e/o Contitolare (eventuale Rappres.nte)	Responsabile	Categoria	Dati sensibili (SI/NO)	Termine ultimo cancell.ne	Categoria	Consenso (SI/NO)	Categoria	Paesi terzi, org.ni int.li (eventuale) (SI/NO)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate