COMUNE DI ACQUALAGNA

Provincia di Pesaro e Urbino

Regolamento comunale per l'attuazione della normativa sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Allegati

A) schema di registro attività di trattamento
B) schema di registro categorie attività di trattamento
C) schema di registro unico di trattamento

Art. 1
Quadro normativo di riferimento

1. Il quadro normativo di riferimento è costituito da:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (RGPD);

- D.lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" per le parti non abrogate o modificate dal D.lgs. 10 agosto 2018 n. 101 (normativa nazionale);

- D.lgs. 10 agosto 2018 n. 101 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 (normativa nazionale);

2. Ai sensi dell'art. 22 comma 1 del D.lgs. 101/2018 le disposizioni de "il presente decreto e le disposizioni dell'ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell'Unione Europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra gli Stati membri ai sensi dell'art. 1, paragrafo 3 del Regolamento (UE) 2016/679".

Art. 2
Glossario Regolamento

1. Ai fini del presente Regolamento, in conformità all'art. 4 del RGPD e nel rispetto del d.lgs. 18/8/2000 n. 267, si intende per:

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;

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;

Titolare del trattamento: l'autorità pubblica (il comune o altro ente locale) che singolarmente o insieme ad altri determina le finalità e le modalità 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 dell'ente titolare;

Soggetto designato per specifici compiti e funzioni ("incaricato" secondo la precedente normativa): il soggetto designato dal Titolare o dal Responsabile che compie attività di trattamento dei dati personali sotto la direzione e l'istruzione di questi ultimi;

Responsabile della Protezione Dati (RPD responsabile protezione dati/ DPO Data Protection Officer): il dipendente del titolare del trattamento o il soggetto che assolve i suoi compiti in base a un contratto di servizi, con funzioni di consulenza dell'Ente, di sorveglianza sul rispetto della normativa e di contatto con l'autorità di controllo;

Responsabile del Sistema Informatico: Il Dirigente / Responsabile di Area/Servizio che per la sua particolare competenza in materia di I.C.T. è designato, da parte del titolare, alla gestione del sistema informatico dell'ente;

Registri delle attività di trattamento*:* elenchi dei trattamenti in forma cartacea o telematica tenuti dal titolare e dal Responsabile del trattamento secondo le rispettive competenze;

DPIA- Data Protection Impact Assessment – Valutazione d'impatto sulla protezione dei dati: procedura finalizzata a descrivere il trattamento, valutarne necessità e

proporzionalità e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali;

Finalità del trattamento*:* esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative che riguardano la popolazione ed il territorio comunale, precipuamente nei settori organici dei servizi alla persona e alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico; la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica; l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate all'Ente; adempimento di un obbligo legale al quale è soggetto l'Ente; esecuzione di un contratto con i soggetti interessati; altre specifiche e diverse finalità;

Misure fisiche, tecniche ed 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; altre misure specifiche adottate per il trattamento di cui trattasi; sistemi di autenticazione, di autorizzazione, di protezione (antivirus, firewall, antintrusione, altro) adottati per il trattamento; misure antiincendio, di rilevazione di intrusione e di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; misure per ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico; procedure per provare, verificare e valutare l'efficacia delle misure tecniche ed organizzative adottate;

Dati particolari: dati inerenti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute, la vita o l'orientamento sessuale (definiti sensibili nella normativa precedente), i dati genetici e biometrici, i dati relativi a condanne penali;

Data breach: qualsiasi violazione di sicurezza dei dati personali 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;

Garante Privacy*:* l'Autorità Garante per la protezione dei dati personali istituita dalla legge 31.12.1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente.

2. Per le altre definizioni qui non riportate o per una definizione più esaustiva si fa riferimento all'art. 4 del RGPD.

Art. 3
Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole specifiche ai fini della migliore funzionalità ed efficacia dell'attuazione della normativa europea e nazionale sulla protezione dei dati personali.

Art. 4
Titolare del trattamento e ripartizione delle competenze tra gli organi del Comune

1.Il **Comune** è titolare dei dati personali raccolti in banche dati automatizzate e/o cartacee.

2. Le attribuzioni del Comune quale titolare del trattamento dei dati personali sono esercitate dai suoi organi secondo la ripartizione che segue.

- il **Consiglio comunale**:

a) emana le norme regolamentari in materia di protezione dei dati personali;

b) stanzia nel bilancio di previsione le risorse finanziarie necessarie per l'efficiente ed efficace esercizio dell'autonomia gestionale da parte dei responsabili interni del trattamento dei dati personali;

c) delibera in ordine alle forme associative ed altri rapporti con soggetti pubblici che comportano la contitolarità del trattamento dei dati personali.

- la **Giunta comunale**:

a) emana le norme regolamentari in materia di ordinamento degli uffici e dei servizi utili per garantire l'efficienza dell'apparato strutturale anche in relazione alla protezione dei dati personali;

b) assicura ai dirigenti / responsabili titolari di posizione organizzativa (P.O.), con il piano esecutivo di gestione le risorse necessarie all'adeguata protezione dei dati personali, anche ai fini, in carenza di professionalità interne, del supporto di specialisti esterni.

- il **Sindaco**:

a) rappresenta il comune nei rapporti con il Garante;

b) designa il responsabile della protezione dei dati personali (RPD);

c) designa, quali soggetti autorizzati al trattamento dei dati personali, per un tempo e per operazioni determinate, gli amministratori comunali ed i funzionari cui abbia rilasciato deleghe o conferito incarichi o che abbiano ricevuto incarichi dal Consiglio o che ne facciano richiesta per l'esercizio del loro potere di indirizzo e di controllo;

d) designa i soggetti autorizzati al trattamento dei dati personali fra gli addetti agli uffici di supporto agli organi di direzione politica;

e) sovrintende sull'osservanza delle disposizioni in materia di trattamento di dati personali;

f) procede alle notifiche ed alle comunicazioni al Garante

- il **Segretario comunale**:

a) coordina i dirigenti/responsabili titolari di posizione organizzativa (p.o.) ai fini dell'applicazione della normativa ed in particolare in ordine agli accordi interni per il trattamento di dati personali gestiti da uffici appartenenti a più settori;

b) coordina i dirigenti/responsabili titolari di posizione organizzativa (p.o.) in ordine alla formazione mirata alla protezione dei dati personali.

- i **Dirigente/Responsabile di posizione organizzativa (p.o.):**

a) ai sensi degli artt. 107 e 109 del d.lgs. 267/2000 esercita le funzioni del Comune titolare del trattamento nell'articolazione organizzativa di propria competenza, con le prerogative e le responsabilità che la legge e la normativa interna all'ente gli attribuisce;

b) E' consentita la designazione di persone autorizzate al trattamento da parte del titolare per specifiche attività di trattamento (definiti "incaricati" nella precedente normativa). Per le operazioni di trattamento i soggetti designati devono attenersi alle istruzioni loro impartite per iscritto, le quali individuano specificatamente l'ambito del trattamento consentito;

c) Il titolare risponde dell'operato dei soggetti designati per specifiche attività di trattamento, anche ai fini del risarcimento di eventuali danni causati dal trattamento stesso, salvo dimostri che l'evento dannoso non è in alcun modo a lui imputabile;

d) Il titolare del trattamento garantisce che chiunque agisce sotto la sua autorità sia in possesso di apposita formazione ed istruzione.

3. I soggetti di cui al comma 2 sono responsabili, ciascuno nell'ambito di propria competenza, del rispetto dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

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 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 alle precedenti lettere, purché l'interessato esprima il consenso al trattamento.

Art.6
Responsabile del trattamento (esterno)

1. Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto dell'ente titolare. I trattamenti da parte del responsabile sono disciplinati da un contratto o da altro atto giuridico che vincola il medesimo al titolare del trattamento e che ne definisce la durata, la natura e la finalità, il tipo di dati personali e le categorie di interessati, gli obblighi ed i diritti del titolare.

2. Il responsabile del trattamento provvede a tutte le attività previste dalla legge ed a tutti i compiti che gli sono affidati. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata da parte del titolare del trattamento;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure tecniche e organizzative per garantire la sicurezza dei trattamenti;

d) ricorra ad un altro responsabile del trattamento solo se autorizzato dal titolare e nel rispetto di tutte le condizioni contenute nel contratto originario tra il titolare e sé medesimo;

e) assista il titolare del trattamento al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
f) assista il titolare negli obblighi di cui all'art 32 e 36 GRPD, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;
g) cancelli o restituisca al titolare del trattamento tutti i dati personali dopo che è terminata la prestazione di cui al contratto e cancelli le copie esistenti;
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GRPD.

3. E' consentita la designazione di persone autorizzate al trattamento da parte del responsabile per specifiche attività di trattamento (definiti "incaricati" nella precedente normativa). Per le operazioni di trattamento i soggetti designati devono attenersi alle istruzioni loro impartite per iscritto, le quali individuano specificatamente l'ambito del trattamento consentito.

4. Il responsabile risponde dell'operato dei soggetti designati per specifiche attività di trattamento anche ai fini del risarcimento di eventuali danni causati dal trattamento stesso, salvo dimostri che l'evento dannoso non è in alcun modo a lui imputabile

Art.7
Responsabile della protezione dati

Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato nella figura unica di un dipendente di ruolo del Comune*, ovvero (in alternativa) di un professionista esterno scelto nel rispetto delle procedure per l'affidamento dei servizi*[1].

[1] *Il RPD può essere scelto fra i dipendenti del Comune di qualifica non inferiore alla cat. D (oppure C negli enti di minore dimensione), purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il Titolare ed il Responsabile del trattamento provvedono affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione. Nel caso in cui il RPD non sia un dipendente dell'Ente, l'incaricato persona fisica è 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*

2. Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza all'Ente, compresi i dipendenti designati per eseguire il trattamento dei dati in merito agli obblighi derivanti dalla normativa relativa alla protezione dei dati. In tal senso il RPD può indicare 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 della normativa relativa alla protezione dei dati. 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;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere nell'Ente;

d)fornire se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il RPD è consultato 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 alla normativa;

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, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Comune al Garante;

f) (eventuale) la tenuta dei registri di cui ai successivi artt. 9 e 10;

---

servizi. Il RPD esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare ed al Responsabile del trattamento. Nel caso di Comuni di minori dimensioni demografiche, è possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più Comuni mediante esercizio associato della funzione nelle forme previste dal d.lgs. 18 agosto 2000 n. 267.

g) altri compiti e funzioni a condizione 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.

3. Il RPD è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

a) è invitato a partecipare alle riunioni di coordinamento dei dirigenti/responsabili p.o. che abbiano per oggetto questioni inerenti la protezione dei dati personali;

b) è reso edotto 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 determini 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.

4. 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.

5. Al RPD sono assicurate autonomia personale nonché risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

6. Il RPD è incompatibile con chi determina le finalità od i mezzi del trattamento, in particolare risultano incompatibili (*in relazione alle dimensioni organizzative del Comune)*:

- il responsabile per la prevenzione della corruzione e per la trasparenza;

- il responsabile del trattamento;

- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

7. Al RPD sono fornite le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare, è assicurato:

- supporto attivo per lo svolgimento dei propri compiti da parte dei dirigenti/responsabili p.o. e della Giunta comunale, a partire dalla programmazione operativa (DUP), dal bilancio, dal peg e dal piano della performance;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero *(in relazione alle dimensioni organizzative dell'Ente)* tramite la costituzione di una unità organizzativa od ufficio;

- 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.

8. 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 per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Sindaco.

Nel caso in cui siano rilevate o sottoposte alla attenzione del RPD decisioni incompatibili con la normativa vigente e con le indicazioni fornite dallo stesso, il medesimo è tenuto a manifestare il proprio dissenso comunicandolo al Sindaco.

Art.8

Sicurezza del trattamento[2]

1. L'Ente mette in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche 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 ed organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono:

- 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 alla normativa 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. L'Ente si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per suo conto ed abbia accesso ai dati personali.

---

[2] *L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.*

6. I nominativi ed i dati di contatto del titolare e del RPD 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.

Art.9
Registro delle attività di trattamento

1. Il registro delle attività di trattamento svolte dal titolare reca almeno le seguenti informazioni:
a) il nome ed i dati di contatto del Comune - titolare del trattamento ed eventualmente dei contitolari, dei responsabili del trattamento e del RPD;
b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.8.

2. Il registro è tenuto dal Comune - titolare ovvero dal soggetto a ciò delegato, presso gli uffici del Comune, in forma telematica/cartacea, secondo lo schema allegato A al presente regolamento; nello stesso possono essere inserite ulteriori informazioni, tenuto conto delle dimensioni organizzative dell'Ente.
3. Il compito di tenere il registro può essere affidato al RPD, ferma restando la responsabilità del titolare.

4. (*in relazione alle dimensioni organizzative del comune)* Il Comune - titolare può decidere di tenere un registro unico dei trattamenti che contiene le informazioni di cui ai commi precedenti e quelle di cui al successivo art. 10, sostituendo entrambe le tipologie di registro dagli stessi disciplinati, secondo lo schema allegato C al presente regolamento.

Art.10
Registro delle categorie di attività trattate

1. Il registro delle categorie di attività trattate reca le seguenti informazioni:

a) il nome ed i dati di contatto del Comune - titolare, ovvero del soggetto a ciò delegato, nonché del RPD;

b) le categorie di trattamenti effettuati: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione e ogni altra operazione applicata a dati personali;

c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.8.

2. Il registro è tenuto presso gli uffici del Comune in forma telematica/cartacea, secondo lo schema allegato B al presente regolamento.

3. Il titolare del trattamento può decidere di affidare al RPD il compito di tenere il registro sotto la propria disponibilità.

Art.11
Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, prima che venga effettuato, deve essere fatta una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi della normativa vigente, 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.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. I criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi, compresa la profilazione e le 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 producono 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 (categorie particolari di dati personali di cui all'art. 9, RGDP);
e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, meritevoli di specifica tutela in quanto posti in una situazione di disequilibrio del rapporto con il titolare/responsabile del trattamento,

come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

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

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati, occorre, in via generale, effettuare una DPIA, salvo che il titolare ritenga motivatamente che non può presentare un rischio elevato; lo stesso può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra, occorra comunque l'effettuazione di una DPIA.

4. Il titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il titolare può affidare l'effettuazione 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 devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA. 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 effettuare una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche;

- 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 precedentemente sottoposto a verifica da parte del Garante 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 o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. La DPIA è condotta prima di dar luogo al trattamento attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei relativi dati, una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;

- del diritto di accesso e portabilità dei dati;

- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;

- dei rapporti con i responsabili del trattamento;

- delle garanzie per i trasferimenti internazionali di dati;

- della consultazione preventiva del Garante.

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento alla normativa vigente, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

9. Il titolare deve consultare il Garante prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il titolare consulta il Garante anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

10. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 12
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 dall'Ente.

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. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Ogni figura coinvolta nella funzione di trattamento è obbligata ad informare il Sindaco, 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 sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;

- perdita del controllo dei dati personali;

- limitazione dei diritti, discriminazione;

- furto o usurpazione d'identità;

- perdite finanziarie, danno economico o sociale.

- decifratura non autorizzata della pseudonimizzazione;

- pregiudizio alla reputazione;

- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il rischio per i diritti e le libertà degli interessati è elevato, questi devono essere informati, senza ingiustificato ritardo, con un linguaggio semplice e chiaro. 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. Il titolare deve documentare le violazioni subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante al fine di verificare il rispetto delle disposizioni vigenti.

Art. 13

Rinvio

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

Approvato con Delibera di Consiglio n. 36 del 2.7.19