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

Approvato con deliberazione C.C. n. 52 / 226 del 17/05/2018

INDICE

Art. 1

Oggetto

1. 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 Alessandria.

Art.2

Titolare del trattamento

1. Il Comune di Alessandria, rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore o suo delegato, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco delega le funzioni di Responsabili del trattamento a Dirigenti/Responsabili di P.O. in possesso di adeguate competenze.

2. Il Titolare o suo delegato 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 o suo delegato mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.

Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

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

4. Il Titolare o suo delegato adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti

presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non 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 o suo delegato deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

6. Il Titolare o suo delegato, inoltre, provvede a:

a) designare i Responsabili del trattamento nelle persone dei Dirigenti/Responsabili di P.O., autorizzando tali Responsabili a individuare i sub-responsabili/incaricati nell'ambito delle singole strutture di riferimento in cui si articola l'organizzazione comunale che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza, al fine di meglio garantire lo svolgimento dei diversificati compiti della struttura comunale. Per il trattamento di dati il Titolare o suo delegato può avvalersi anche di soggetti pubblici o privati;

b) nominare il Responsabile della protezione dei dati – RPD, la cui figura è obbligatoriamente prevista per le autorità pubbliche o organismi pubblici;

c) nominare quali Responsabili del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 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, nonché 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 o suo delegato e dei Responsabili del trattamento.

Art.3

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 utilizzo 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 e la finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

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

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

Art.4

Responsabili del trattamento

1. I Dirigenti dell'Ente assegnati ai Settori di *line* e di *staff*, nonché i Dirigenti/Responsabili di P.O. assegnati a Servizi Autonomi sono nominati Responsabili del trattamento di tutte le banche dati personali esistenti nell'ambito del Settore/Servizio (indipendentemente dalla denominazione) di riferimento e di rispettiva competenza. I Responsabili collaborano con il Titolare o suo delegato e con il Responsabile della protezione dei dati - RPD per individuare le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.

2. I dipendenti del Comune, Responsabili del trattamento, sono designati, di norma, mediante decreto di incarico del Sindaco, dal quale, essendo individuato il Settore e i Servizi di assegnazione, risultano:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;

- il tipo di dati personali oggetto di trattamento e le categorie di interessati;

- gli obblighi ed i diritti del Titolare o suo Delegato del trattamento.

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun Responsabile designato.

3. Il Titolare o suo delegato può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 RGPD, stipulando atti giuridici in forma scritta, che specificano 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. Gli atti che disciplinano il rapporto tra il Titolare e i Responsabili del trattamento devono in particolare contenere quanto previsto dall'art. 28, punto 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

5. Il Titolare autorizza la nomina di sub-responsabili/incaricati del trattamento da parte di ciascun Responsabile del trattamento nell'ambito delle singole strutture di riferimento in cui si articola l'organizzazione comunale che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza, sempre nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da sub-responsabili/incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificamente l'ambito del trattamento consentito.

I Responsabili rispondono, anche dinanzi al Titolare o suo delegato, dell'operato dei sub-responsabili/incaricati anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostrino che l'evento dannoso non sia in alcun modo loro imputabile e che hanno vigilato in modo adeguato sull'operato dei sub-responsabili/incaricati.

6. I Responsabili del trattamento garantiscono che chiunque agisca sotto la loro autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

7. I Responsabili del trattamento dei dati collaborano direttamente e/o attraverso

specifici referenti da loro stessi individuati, per il proprio ambito di competenza, con il Titolare o suo delegato e con il RPD a tutte le attività previste dalla legge con particolare riferimento a:

- tenuta dei registri delle categorie di attività di trattamento svolte per conto del Titolare e delle attività di trattamento;
- attuazione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- sensibilizzazione e promozione della formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- assistenza al Titolare o suo delegato nella conduzione della valutazione dell'impatto sulla protezione dei dati - DPIA fornendo allo stesso ogni informazione di cui è in possesso;
- informare il Titolare o suo delegato, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso o suo delegato ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art.5

Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato e nominato dalla Giunta Comunale nella figura unica di un dipendente a tempo indeterminato dell'Ente che non sia Responsabile del trattamento di dati, in rapporto alle funzioni di riferimento trasversali a tutta la struttura e alla conoscenza specialistica in materia di protezione e sicurezza dei dati, oppure di un professionista esterno in possesso di tutte le qualità professionali atte a ricoprire il ruolo (approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili, oltre che una conoscenza specialistica adeguata e correlata a specifica formazione periodicamente aggiornata in materia di protezione e sicurezza dei dati) scelto mediante una procedura ad evidenza pubblica.
In particolare il RPD deve possedere una comprovata conoscenza specialistica della normativa e della prassi in materia di protezione e di sicurezza delle banche dati, nonché la capacità di promuovere la diffusione di una cultura della protezione e della sicurezza dei dati all'interno dell'organizzazione comunale, favorendo la formazione del personale dell'Ente attraverso la proposta di piani di aggiornamento periodico.

2. Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare o suo delegato e ai Responsabili del trattamento, nonché ai dipendenti sub-responsabili/incaricati che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare o suo delegato e/o ai Responsabili 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, nonché a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare o suo delegato e dei Responsabili del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare o suo delegato e dei Responsabili del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare o suo delegato e dai Responsabili del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare o suo delegato, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

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

f) tenuta dei registri di cui ai successivi artt. 7 e 8;

g) altri compiti e funzioni a condizione che il Titolare o suo delegato, coadiuvato dai Responsabili del trattamento, si assicuri 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 Titolare o suo delegato e i Responsabili del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, allo scopo di creare una positiva e costruttiva sinergia interna che favorisca la condivisione di problematiche e soluzioni operative. A tal fine:

- il RPD partecipa alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. di Settori/Servizi Autonomi che abbiano per oggetto questioni inerenti alla protezione e sicurezza dei dati personali;

- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti a decisioni che impattano sulla protezione e sicurezza 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, in quanto collabora e supporta il Titolare o suo delegato e i Responsabili del trattamento rispetto agli adempimenti previsti dall'art. 33 RGPD.

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 e sicurezza dei dati, redigendo il Privacy Impact Assessment – PIA finalizzato alla valutazione dei rischi privacy e all'individuazione di un piano per ridurli;

b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare o suo delegato e ai Responsabili del trattamento.

5. Il RPD dispone di autonomia e risorse economiche e umane sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente, operando in modo trasversale all'interno della struttura organizzativa complessa dell'Ente.

6. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

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

trattamento.

7. Il Titolare o suo delegato e i Responsabili del trattamento forniscono al RPD tutte le informazioni e la collaborazione necessarie per favorire lo svolgimento dei compiti di riferimento e per accedere ai dati personali e ai trattamenti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte del Titolare o suo delegato, dei Dirigenti/Responsabili P.O. e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione e messa in sicurezza dei dati nell'ambito della programmazione operativa (DUP), di bilancio e di PEG;

- tempo sufficiente per l'espletamento dei compiti affidati al RPD;

- supporto adeguato in termini di risorse finanziarie, umane, infrastrutture (sede, attrezzature, strumentazione), con la possibilità di prevedere anche la costituzione di Unità di progetto interna a supporto del RPD per specifiche finalità (ad es. per la tenuta dei registri delle attività di trattamento e delle categorie di attività);

- 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 dal Titolare del trattamento per l'adempimento dei propri compiti.

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

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

Art.6

Sicurezza del trattamento

1. Il Comune di Alessandria, nella persona del Titolare - Sindaco o suo delegato, e

ciascun Responsabile del trattamento collaborano con il RPD per attuare le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio tenendo conto della programmazione definita dal RPD in base allo stato dell'arte e alle risorse economiche a disposizione per coprire i costi di attuazione, nonché rispetto alla natura, al campo di applicazione, al contesto e alle finalità del trattamento, come anche in considerazione del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (distruzione, perdita, modifica, divulgazione non autorizzata o 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 (fase realizzativa).

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

3. Costituiscono misure tecniche (da attuare con il supporto di risorse del sistema informativo di Ente e della struttura economale e/o di altre strutture interne) ed organizzative che possono essere adottate dal Settore/Servizio Autonomo cui è preposto ciascun Responsabile del trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);

- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

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

5. Il Comune di Alessandria e ciascun Responsabile del trattamento, con il supporto del RPD, forniscono adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare o suo delegato, dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente esistente o che il RPD valuterà di attivare.

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

Art.7

Registro delle attività di trattamento

1. Ai sensi dell'art. 30 RGPD è istituito il Registro delle attività di trattamento svolte dal Titolare del trattamento o suo delegato e reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto del Comune, del Titolare del Trattamento (Sindaco pro tempore o di suo delegato), eventualmente del Contitolare del trattamento, 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.6.

2. Il Registro, salvo disposizioni diverse del Titolare del trattamento o suo delegato, è tenuto dal RPD, sotto la responsabilità del Titolare medesimo o suo delegato, presso gli uffici della struttura organizzativa di *staff* cui il RPD è assegnato e comunque, in caso di titolarità in capo ad un professionista esterno (ai sensi del precedente art. 5, punto 1), presso il Servizio Autonomo Sistemi informativi ed e-government del Comune in forma telematica/cartacea, secondo lo schema allegato A al presente Regolamento, suscettibile di integrazioni che in corso d'opera si rendessero necessarie, riportando lo stesso i dati minimi utili.

Art.8

Registro delle categorie di attività trattate

1. Ai sensi dell'art. 30 RGPD è istituito il Registro delle categorie di attività trattate da ciascun Responsabile di cui al precedente art. 4 e reca le seguenti informazioni:

a) il nome ed i dati di contatto del Comune, del Titolare del Trattamento (Sindaco pro tempore o di suo delegato), dei Responsabili del trattamento e del RPD;
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 od una organizzazione internazionale;

d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il registro è tenuto dal RPD, sotto la responsabilità di ciascun Responsabile del trattamento, presso gli uffici della struttura organizzativa di *staff* cui il RPD è assegnato e comunque, in caso di titolarità in capo ad un professionista esterno (ai sensi del precedente art. 5, punto 1), presso il Servizio Autonomo Sistemi informativi ed e-government del Comune in forma telematica/cartacea, secondo lo schema allegato B al presente Regolamento, suscettibile di integrazioni che in corso d'opera si rendessero necessarie, riportando lo stesso i dati minimi utili.

Art.9

Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, soprattutto 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 o suo delegato, 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, adeguatamente supportato dal RPD. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'at. 35, punti da 4 a 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, punto 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

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

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

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

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

e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

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

g) dati relativi a interessati vulnerabili, ossia 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 o suo delegato, 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, condurre una DPIA, salvo che il Titolare o suo delegato ritenga motivatamente che non può presentare un rischio elevato; il Titolare o suo delegato può motivatamente ritenere che per un trattamento che soddisfa anche solo uno dei criteri di

cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare o suo delegato garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare o suo delegato di regola affida la conduzione materiale della DPIA al RPD che si avvale della collaborazione dei Responsabili del trattamento e/o dei loro referenti, potendo, qualora lo reputi necessario, avvalersi di un soggetto esterno al Comune, scelto mediante una procedura ad evidenza pubblica.

Il Titolare o suo delegato 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 o suo delegato devono essere documentate nell'ambito della DPIA. Il RPD svolge direttamente ovvero monitora lo svolgimento della DPIA, a seconda di quanto indicato al precedente capoverso.

Il/I Responsabile/i del trattamento deve/devono assistere il Titolare o suo delegato nella conduzione della DPIA fornendo ogni informazione necessaria.

Il responsabile della sicurezza dei sistemi informativi e/o l'ufficio competente per detti sistemi forniscono supporto al Titolare o suo delegato 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 e/o l'ufficio competente per detti sistemi possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

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 ai sensi dell'art. 35, punto 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 RPD e che proseguano con

le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

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 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, soppesando 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 singola tipologia di 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.

8. Il Titolare o suo delegato 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 o suo delegato 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 o suo delegato consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

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. 10

Violazione dei dati personali

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

2. Il Titolare o suo delegato, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e, comunque, senza ingiustificato ritardo. Il/I Responsabile/i del trattamento è/sono obbligato/i ad informare il Titolare o suo delegato, senza ingiustificato ritardo, dopo essere venuto/i a conoscenza della violazione. Il RPD supporta Titolare o suo delegato e i Responsabili del trattamento nella succitata notifica, al fine di garantirne la tempestività.

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 Titolare o suo delegato ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro, al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;

- riguardare categorie particolari di dati personali;

- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);

- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);

- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

6. Il Titolare o suo delegato deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD. A tal fine detta documentazione viene conservata dal RPD presso gli uffici della struttura organizzativa di *staff* cui il RPD è assegnato e comunque, in caso di titolarità in capo ad un professionista esterno (ai sensi del precedente art. 5, punto 1), presso il Servizio Autonomo Sistemi informativi ed e-government del Comune in forma telematica/cartacea.

Art.11

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.

ALLEGATI

A) Registro attività di trattamento

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**	

	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

REGISTRO CATEGORIE DI ATTIVITA' DI TRATTAMENTO (art. 30, c.2, GPRD)			
ENTE TITOLARE DEL TRATTAMENTO		**Responsabile del trattamento**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
		Registro tenuto da	
		Data di creazione	
		Ultimo aggiornamento	
		N. schede compilate	
		Prossima revisione	

	TRATTAMENTO				TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Categorie	eventuale diverso Titolare e/o Contitolare (eventuale Rappres.nte)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

GLOSSARIO REGOLAMENTO

Ai fini del presente testo regolamentare comunale, si intende per:

- **Titolare del trattamento**

  l'autorità pubblica (il Comune e per esso il Sindaco pro tempore o suo delegato) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.

- **Responsabile del trattamento**

  il Dirigente/Responsabile P.O., oppure il soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.

- **Sub-Responsabile/incaricato del trattamento**

  il dipendente della struttura organizzativa del Comune, incaricato dal Responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento (elabora o utilizza materialmente i dati personali).

- **Responsabile per la protezione dati – RPD**

  il dipendente della struttura organizzativa di *staff* del Comune, il professionista privato o impresa esterna, incaricati dal Titolare del trattamento.

- **Registri delle attività di trattamento**

  elenchi dei trattamenti in forma cartacea o telematica tenuti dal RPD sotto la responsabilità del Titolare del trattamento.

- **Registri delle categorie di attività di trattamento**

  elenchi delle categorie di trattamenti in forma cartacea o telematica tenuti dal RPD sotto la responsabilità dei Responsabili del trattamento secondo le rispettive competenze.

- **DPIA - Data Protection Impact Assessment - Valutazione d'impatto sulla protezione dei dati**

  è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

- **Garante Privacy**

  il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 675, quale autorità amministrativa pubblica di controllo indipendente.

GLOSSARIO REGISTRI

Ai fini degli schemi dei registri, si intende per:

❖ Categorie di trattamento

Raccolta; registrazione; organizzazione; strutturazione; conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto od interconnessione; limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.

❖ Categorie di dati personali

Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo *on-line* (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale.
Dati inerenti lo stile di vita
Situazione economica, finanziaria, patrimoniale, fiscale.
Dati di connessione: indirizzo IP, login, altro.
Dati di localizzazione: ubicazione, GPS, GSM, altro.

❖ Finalità del trattamento

Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti alla popolazione e al territorio, nei settori organici dei servizi alla persona, 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.
Adempimento di un obbligo legale al quale è soggetto il Comune.
Esecuzione di un contratto con i soggetti interessati.
Altre specifiche e diverse finalità.

❖ Misure 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; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi.

Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) adottati per il trattamento di cui trattasi ovvero dal Settore/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 Settore/Servizio/Ente nel suo complesso.

Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

❖ Dati sensibili

Dati inerenti all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, all'appartenenza sindacale, alla salute, alla vita o all'orientamento sessuale, dati genetici e biometrici, dati relativi a condanne penali.

❖ Categorie interessati

Cittadini residenti; minori di anni 16; elettori; contribuenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; altro.

❖ Categorie destinatari

Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.