COMUNE DI CALTRANO

PROVINCIA DI VICENZA

REGOLAMENTO SULLA PROTEZIONE DEI DATI PERSONALI

PER L'ATTUAZIONE DEL REGOLAMENTO UE N. 2016/679

Approvato con deliberazione di C.C. n. 15 del 30.03.2019

Sommario

TITOLO I - PRINCIPI

Art. 1. Oggetto

1.1 Il presente Regolamento (di seguito il "Regolamento") ha per oggetto le misure procedimentali ed i processi interni di attuazione del Regolamento EU 679/16 ("Regolamento generale sulla protezione dei dati", di seguito "GDPR") e del D. Lgs. n. 196/2003 ("Codice in materia di protezione dei dati personali", di seguito "Codice Privacy"), **modificato dal D.Lgs. n. 101/2018**, ai fini del trattamento dei dati personali per le finalità istituzionali del Comune di Caltrano.

Art. 2. Principi del trattamento

2.1 Nel rispetto dell'art. 5 GDPR, i dati saranno:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza);

b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità ("limitazione della finalità);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione");

d) esatti e, se necessari, aggiornati ("esattezza");

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, salvo le esigenze di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, in conformità all'art. 89, paragrafo 1, GDPR ("limitazione della conservazione");

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

2.2 I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati sono inutilizzabili.

Art. 3. Definizioni

Ai fini del presente Regolamento si adottano le seguenti definizioni:

- dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente;

- dati particolari: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi ad individuare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 GDPR);
- dati giudiziari: dati relativi a condanne penali e a reati ai sensi dell'art. 10 GDPR;
- 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;
- archivio: qualsiasi insieme di dati accessibili secondo criteri determinati, indipendentemente dal fatto che tale archivio sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- titolare del trattamento: il Comune, il quale determina le finalità e i mezzi del trattamento dei dati personali:
- responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- autorizzato/designato al trattamento: la persona fisica che è autorizzata a trattare dati personali sotto l'autorità del titolare del trattamento;
- responsabile della protezione dei dati: soggetto designato ai sensi degli articoli 37 e seguenti GDPR;
- destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali;
- terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate;
- Garante: il Garante per la protezione dei dati personali.

TITOLO II - SOGGETTI DEL TRATTAMENTO DATI

Art. 4. Titolare del trattamento

4.1 Il Comune di **Caltrano,** nella persona del Sindaco, è il titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito il "Titolare" o il "Comune").

4.2 Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

4.3 Il Titolare deve mettere in atto le 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 GDPR. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa di bilancio, 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.

4.4 Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non stati ottenuti presso lo stesso interessato.

4.5 Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA"), ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 15.

4.6 Il Titolare, inoltre, provvede a:

a) nominare ai sensi dell'art. 29 GDPR e dell'art. 2 *quaterdecies* del Codice Privacy i designati autorizzati al trattamento nelle persone dei Responsabili dei vari Settori nonché dei dipendenti dei singoli Uffici in cui si articola l'organizzazione comunale; tali soggetti sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza, con funzioni e compiti corrispondenti al ruolo ed all'inquadramento di ciascuno.

b) nominare il Responsabile della protezione dei dati ai sensi dell'art. 37 GDPR;

c) nominare quali Responsabili del trattamento ai sensi dell'art. 28 GDPR 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;

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

4.8 Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 5. Designati – autorizzati al trattamento

5.1 Il Titolare del trattamento nomina, con decreto del Sindaco o con diverso atto ritenuto opportuno, i designati al trattamento dei dati personali ai sensi dell'art. 29 GDPR e art. 2 *quaterdecies* Codice Privacy, attribuendo specifiche funzioni, in base ai rispettivi ruoli.

5.2 I Responsabili dei vari Settori, in considerazione delle conoscenze specialistiche, dell'esperienza, della capacità ed affidabilità, dovranno:

a) vigilare sulla corretta applicazione del GDPR e del Codice Privacy da parte del personale autorizzato del proprio Settore, comunicando al Titolare del trattamento e al Responsabile della Protezione dei dati gli eventuali nuovi trattamenti da svolgere, provvedendo alle necessarie misure di sicurezza;

b) provvedere alla tenuta e implementazione del Registro delle attività di trattamento di cui all'art. 30 GDPR, secondo le istruzioni ricevute dal Titolare del trattamento;

c) in tutti i casi in cui il Comune affidi a un soggetto esterno all'Amministrazione operazioni di trattamento di dati per conto del Comune, provvedere a formalizzare la nomina a "responsabile del trattamento" ai sensi dell'art. 28 GDPR, di concerto con il Responsabile della Protezione dei dati e con il Titolare del trattamento;

e) ricevere e gestire le richieste di esercizio dei diritti da parte degli interessati di cui agli articoli 15-22 GDPR, ove applicabili, relativamente al Settore di appartenenza;

f) tenere traccia del percorso logico e delle motivazioni che hanno comportato una determinata scelta in materia di privacy;

g) verificare periodicamente, con il supporto del Responsabile della Protezione dei dati, l'adeguatezza delle misure di sicurezza adottate, valutando il livello di rischio inerente al trattamento e l'eventuale necessità di

adottare misure più adeguate, di concerto con il Titolare del trattamento e con il Responsabile della Protezione dei dati;

h) interagire con i soggetti incaricati di eventuali verifiche, controlli e ispezioni, evadendo tempestivamente le richieste di informazioni da parte dell'Autorità Garante, dando immediata esecuzione alle eventuali indicazioni che pervengano dall'Autorità stessa;

5.3 I dipendenti dei vari Uffici comunali, diversi dai Responsabili dei Settori di cui al punto 5.2, in qualità di designati - autorizzati al trattamento dei dati potranno trattare i dati personali per le finalità proprie dell'Ufficio di appartenenza, nonché accedere alle banche dati relative al proprio Ufficio, nel rispetto delle disposizioni del GDPR, del Codice Privacy e di tutte le altre norme di legge.

Art. 6. Responsabili del trattamento

6.1 Il Titolare può avvalersi di soggetti pubblici o privati che, in qualità di Responsabili del trattamento, effettuino dei trattamenti di dati personali, anche particolari, per conto del Titolare. Tali soggetti devono essere nominati tra soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

6.2 Il Responsabile del trattamento è designato, di norma, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

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

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

- gli obblighi ed i diritti del Titolare del trattamento.

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

6.3 Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, paragrafo, 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

6.4 Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

Art. 7. Responsabile della protezione dei dati

7.1. Il Comune deve provvedere alla nomina del Responsabile della protezione dei dati (di seguito "DPO"). La nomina del DPO deve essere comunicata al Garante per la protezione dei dati personali, con le procedure previste, nonché a tutti i dipendenti del Comune, in modo che sia nota a tutti la sua presenza e funzione. Il

nominativo nonché i recapiti del DPO devono essere pubblicati nel sito del Comune nella sezione "Amministrazione Trasparente" o in apposita sezione.

7.2 Il DPO è tenuto a:

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

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare. 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;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il DPO 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 GDPR;

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 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione;

f) fornire un parere al Titolare in caso di violazione dei dati personali per valutare la gravità del "*data breach*".

Il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificamente tale decisione.

7.3 Il Titolare assicura che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il DPO è invitato a partecipare alle riunioni di coordinamento dei Responsabili dei Settori che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- il DPO deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

- il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

7.4 Il Titolare fornisce al DPO le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al DPO:

- supporto attivo per lo svolgimento dei compiti da parte dei Responsabili dei Settori e della Giunta comunale,

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

- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;

- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno del Comune;

- accesso garantito ai settori funzionali del Comune così da fornirgli supporto, informazioni e input essenziali.

7.5 Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti. Non deve ricevere istruzioni in merito ai compiti da svolgere né sull'interpretazione da dare ad una specifica questione in merito alla protezione dei dati. Il DPO non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti. Nello svolgimento del proprio incarico, il DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

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

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

TITOLO III – TRATTAMENTO DEI DATI PERSONALI

Art. 8. Trattamento dei dati particolari e dei dati giudiziari

8.1 Gli Uffici del Comune trattano anche dati particolari come definiti dall'art. 9 GDPR e dall'art. 3 del presente Regolamento. In conformità all'art. 9, paragrafo 2, del GDPR, il Comune tratta i dati particolari per le seguenti finalità:

- per motivi di interesse pubblico rilevante, come specificato nell'art. 12 del presente Regolamento;

- per tutelare un interesse vitale dell'interessato di altra persona fisica qualora l'interessato si trovi nella incapacità fisica o giuridica di prestare il proprio consenso;

- per assolvere gli obblighi ed esercitare i diritti specifici del Titolare o dell'interessato in materia di diritto del lavoro o della sicurezza e protezione sociale, nella misura autorizzata dalla legge o dalla contrattazione collettiva;

- il trattamento riguarda dati resi manifestamente pubblici dall'interessato;

- il trattamento è necessario ai fini dell'archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ed è proporzionato alle finalità perseguite;

- l'interessato ha prestato il proprio consenso esplicito al trattamento per una o più finalità specifiche.

I dati particolare relativi alla salute non possono essere diffusi.

8.2 Il trattamento di dati giudiziari può avvenire solo sotto l'autorità pubblica o, negli altri casi, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati, ai sensi dell'art. 2 *octies* del Codice Privacy.

8.3 I dati particolari ed i dati giudiziari sono trattati sempre nel rispetto dei principi di cui all'art. 2 del presente Regolamento.

Art. 9. Individuazione dei settori di interesse pubblico rilevante

9.1 I trattamenti di dati particolari ex art. 9 GDPR, necessari per motivi di interesse pubblico rilevante, sono ammessi quando previsti da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino che tipo di dati possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

9.2 Fermo restando quanto previsto dall'articolo precedente, si considera rilevante l'interesse pubblico relativo alle seguenti materie, ai sensi dell'art. 2 *sexies*, comma 2, Codice Privacy, sono i seguenti:

a) accesso a documenti amministrativi e accesso pubblico;

b) tenuta degli atti e dei registri dello stato civile, delle anagrafe della popolazione residente in Italia e dei cittadini italiani all'estero, delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o di cambiamento delle generalità;

c) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;

d) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali e assembleari;

e) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;

f) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;

g) attività di controllo e ispettive;

h) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;

i) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessioni di patrocini, patronati e premi di rappresentanza, adesione a comitati e ammissione a cerimonie ed incontri istituzionali;

l) rapporti tra i soggetti pubblici e gli enti del terzo settore;

m) obiezioni di coscienza;

n) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;

o) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;

p) attività socio assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;

q) istruzione e formazione in ambito scolastico e professionale;

r) trattamenti effettuati ai fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato, negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

s) instaurazione, gestione ed estinzione di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

Art.10. Registro delle attività di trattamento

10.1 Il Titolare del trattamento istituisce e tiene aggiornati, in forma scritta ed in formato elettronico, tramite i designati al trattamento di cui all'art. 5 del presente Regolamento, i registri delle attività di trattamento di cui all'art. 30 GDPR. I registri dovranno essere predisposti per ogni Settore e dovranno essere costantemente aggiornati e messi a disposizione del Garante.

10.2 Nei registri dovranno essere indicate le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento e del DPO;

b) le finalità del trattamento;

c) la descrizione delle categorie di interessati e delle categorie di dati personali;

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

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo od organizzazione internazionale;

f) ove applicabile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'art. 32 GDPR.

10.3 Tale registro dovrà essere tenuto anche dai Responsabili del trattamento.

Art. 11. Pubblicazione nel sito istituzionale del Comune per obblighi di trasparenza

11.1 Il Comune provvede a pubblicare nel suo sito internet i dati la cui pubblicazione sia prevista per obblighi di trasparenza ai sensi del d.lgs. n. 33/2013 "*Riordino della disciplina riguardante il diritto di accesso civico e agli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*" e delle "*Linee Guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*" pubblicate sulla Gazzetta Ufficiale n. 134 del 12.06.2014.

11.2 I documenti contenenti atti oggetto di pubblicazione obbligatoria devono tempestivamente e devono essere costantemente aggiornati. Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con le finalità di pubblicazione.

11.3 I dati particolari o giudiziari possono essere diffusi solo se indispensabili; i dati relativi alla salute non possono essere diffusi.

11.4 I dati vanno pubblicati in formato aperto ai sensi dell'art. 68 del D. Lgs. n. 82/2005 e sono riutilizzabili senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità, nel rispetto della normativa vigente.

11.5 I dati, le informazioni e i documenti oggetto di pubblicazione obbligatoria ai sensi del comma 1 del presente articolo sono pubblicati per un periodo di 5 (cinque) anni decorrenti dal 1° gennaio dell'anno successivo a quello dell'obbligo di pubblicazione, e comunque fino a che gli atti producono i loro effetti, ad eccezione:

- dei diversi termini previsti dalla normativa sulla protezione dei dati personali;

- di alcuni dati e informazioni riguardanti i titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale e regionale e locale ai sensi dell'articolo 14, comma 2, d.lgs. 33/2013 e i titolari di incarichi dirigenziali e di collaborazione o consulenza che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell'incarico ai sensi dell'art. 15, comma 4, D. Lgs. n. 33/2013.

11.6 I dati personali devono essere conservati, in ogni caso, nel rispetto del principio della minimizzazione dei dati. Di conseguenza, l'interessato ha diritto ad ottenere la cancellazione dei dati personali di cui non è più necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.

TITOLO IV- MISURE DI SICUREZZA

Art. 12. Misure di sicurezza per trattamenti con strumenti elettronici ed informatici

12.1 Il Comune mette in atto misure tecniche ed organizzative adeguate 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. Il Titolare del trattamento, nel predisporre tali misure di sicurezza, si è uniformato alle misure minime di sicurezza previste nella Circolare 18 aprile 2017 n. 2/2017 dell'Agenzia per l'Italia Digitale. Il Titolare ha istruito in forma scritta tutto il personale del

Comune autorizzato al trattamento dei dati personali a rispettare le predette misure di sicurezza, che prevedono:

- attribuzione agli autorizzati di credenziali di autenticazione, composte da un nome utente e da una parola chiave (password) composta da almeno 8 caratteri, oppure nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;

- modifica della password al primo utilizzo ed in seguito almeno ogni sei mesi o tre mesi in caso di trattamento di dati particolari;

- disattivazione delle credenziali di autenticazione in caso di perdita della qualifica di autorizzato o di mancato utilizzo per un periodo superiore a 6 mesi;
- protezione degli elaboratori contro i rischi di intrusione, mediante appositi programmi (antivirus, firewall, ecc.);
- verifica dell'efficacia e dell'aggiornamento del software antivirus, almeno con cadenza settimanale;
- distruzione dei supporti di memorizzazione nel caso non siano riutilizzabili, mediante procedura certificata;
- sistemi di copiatura e conservazione di archivi elettronici, misure idonee a ripristinare tempestivamente la disponibilità dei dati e l'accesso in caso di incidente fisico o tecnico.

12.2 Il Comune favorisce l'adesione ai codici di condotta elaborati da associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrare il concreto rispetto da parte del Titolare e dei Responsabili del Trattamento.

Art. 13. Misure di sicurezza per trattamenti eseguiti senza l'ausilio di strumenti elettronici.

13.1 Il Comune ha fornito per iscritto agli autorizzati al trattamento dei dati le istruzioni da seguire durante le operazioni di trattamento di atti e documenti contenenti dati personali senza l'ausilio di strumenti elettronici, di seguito riportate:

- i documenti contenenti dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali; in questo caso, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- per tutto il periodo in cui i documenti contenenti dati personali sono al di fuori dei locali individuati per la loro conservazione, anche all'esterno del posto di lavoro, l'autorizzato non dovrà mai lasciarli incustoditi e dovrà tenere sempre con se la borsa o la cartella contenenti i documenti;
- l'autorizzato deve evitare che terzi non autorizzati possano esaminare anche solo la copertina del documento in questione;
- l'autorizzato dovrà verificare costantemente l'integrità e la completezza dei raccoglitori che contengano documenti recanti dati personali;
- al termine dell'orario di lavoro, l'autorizzato dovrà riporre i documenti contenenti dati personali nei locali individuati per la loro conservazione;

- i documenti contenenti dati personali non devono mai essere lasciati incustoditi sul tavolo durante l'orario di lavoro;
- deve essere limitato l'utilizzo di copie fotostatiche, in modo da evitare il rischio di diffusione di dati;
- nel caso vi siano fotocopiatori collocati in aree accessibili al pubblico, l'autorizzato deve prelevare le copie effettuate nel più breve tempo possibile, evitando di lasciarle incustodite;
- è necessario adottare particolari cautele nel caso in cui l'autorizzato consegni ad altro autorizzato documenti in originale;
- i documenti contenenti dati particolari, dati giudiziari o comunque meritevoli di particolare attenzione, devono essere custoditi con estrema cura e conservati in armadi e/ cassetti chiusi a chiave. L'accesso agli archivi contenenti i predetti dati deve essere controllato;
- è vietato utilizzare all'esterno del luogo di valoro copie fotostatiche di documenti di identità (anche se non perfettamente riuscite) come carta riciclata;
- è proibito discutere, comunicare o trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a poter trattare i dati in questione;
- è opportuno che l'autorizzato non parli ad alta voce, trattando dati per telefono, soprattutto al cellulare, in presenza di terzi non autorizzati, per evitare che questi possano prendere conoscenza, anche accidentale, dei dati, soprattutto in luogo pubblico o aperto al pubblico;
- le persone ammesse, dopo l'orario di chiusura, sono identificate e registrate e se mancano strumenti elettronici di controllo degli accessi agli archivi, questi vanno preventivamente autorizzati.

Art. 14. Misure per dati raccolti con i sistemi di videosorveglianza

14.1 I dati raccolti mediante sistemi di videosorveglianza sono protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita anche accidentale, modifica, divulgazione non autorizzata o accesso in modo accidentale o illegale, trattamento non consentito o non conforme alle finalità della raccolta.

14.2 E' necessario rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo le immagini indispensabili, limitando l'angolo della visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.

14.3 Nel rispetto del Provvedimento in materia di videosorveglianza del Garante di data 08.04.2010 (pubblicato nella Gazzetta Ufficiale n. 99 del 29.04.2010), devono essere adottate le seguenti specifiche misure tecniche ed organizzative:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori, devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base

alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati autorizzati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;

b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;

c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;

d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;

e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo.

14.4 Il Comune provvede all'installazione della adeguate informative in modo da fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, ai sensi dell'art. 21 del presente Regolamento. Per ogni ulteriore informazione si rimanda al Regolamento Comunale per la disciplina delle videosorveglianza.

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

15.1 Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Comune, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, 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.

15.2 La DPIA può riguardare una sola operazione di trattamento o duo o più trattamenti simili che presentino rischi elevati analoghi.

15.3 Ai sensi dell'art. 35, paragrafo 3, GDPR, la DPIA è richiesta in presenza di:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, paragrafo 1, GDPR o di dati relativi a condanne penali e a reati di cui all'art. 10 GDPR;

c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

15.4. Fermo restando quanto indicato dall'art. 35, paragrafo 3, GDPR, 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 GDPR;

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, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti del Comune, 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 ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

15.5 Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.

Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA.

Qualora il trattamento viene eseguito in tutto o in parte da un responsabile del trattamento, quest'ultimo deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'Amministratore di Sistema, forniscono supporto al Titolare per lo svolgimento della DPIA.

15.6 Il DPO 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 informatici, se nominato, e/o l'Amministratore di Sistema, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

15.7 La DPIA non è necessaria nei casi seguenti:

- ✓ se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, GDPR;
- ✓ 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 per la protezione dei dati personali prima del maggio 2018, in condizioni specifiche che non hanno subito modifiche;
- ✓ se un trattamento, effettuato per adempiere un obbligo legale del titolare e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, 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.

Inoltre, occorre tenere 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.

15.8 La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento,

i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

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

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante;

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

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

15.9 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.

15.10 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.

15.11 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. 16. Violazione dei dati personali

16.1 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.

16.2 Nel caso in cui si verifichi un'ipotesi di data breach, il Titolare dovrà seguire tutte le istruzioni riportate nel "*Protocollo in caso di violazione dei dati personali ai sensi degli articoli* 33 e seguenti del Regolamento UE 679/16 ("Regolamento generale sulla protezione dei dati**")"**

Art. 17. Sistema e politica di audit

17.1 Il Comune ha messo in atto misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è conforme al GDPR e al Codice Privacy e a tal fine, ha adottato un procedimento di Audit, coadiuvato dal DPO e dai consulenti esterni nominati in materia di privacy, volto a:

- verificare il grado di conformità alla normativa vigente del trattamento dei dati personali effettuato da tutti gli Uffici del Comune;

- verificare che tutti i dipendenti osservino le regole per la liceità e la sicurezza del trattamento dei dati personali;

- verificare l'efficacia delle azioni correttive a seguito di "non conformità".

Il processo consiste:

- in una prima mappatura delle possibili situazioni di rischio che si verificano nel Comune, tenuto conto dell'organizzazione del Comune nei vari Uffici e del trattamento dei dati svolto in ciascuno;
- nell'individuare situazioni di non conformità del trattamento agli standard di sicurezza adeguati al rischio;
- nel porre in essere le azioni correttive.

Il processo, dopo la sua prima ultimazione, si sviluppa in monitoraggi periodici volti a verificare l'effettiva applicazione delle misure stabilite e nel riesame e nella sostituzione delle misure, al fine di permettere un costante adeguamento alla normativa vigente.

17.2 Nel concreto, l'Audit si svolgerà mediante:

- interviste dirette e/o sottoposizione di questionari agli autorizzati al trattamento dei dati;

- verifiche dei sistemi informatici.

A seguito delle attività precedenti, vengono analizzati i risultati emersi che possono consistere in:

- situazioni di conformità;

- raccomandazioni per il miglioramento;

- situazioni di non conformità.

I risultati verranno formalizzati in un rapporto di Audit nel quale verrà dato atto di tutte le fasi del procedimento svolto, fornendo al Comune l'indicazione delle eventuali misure correttive da adottare.

Art. 18. Verifiche periodiche

18.1 Il Comune, tramite i Responsabili dei Settori, verifica almeno ogni sei mesi che vengano applicate le procedure interne e le misure di sicurezza adottate in sede di Audit, sia relative ai trattamenti con strumenti informatici che con modalità cartacee. In caso di riscontro di non corretta applicazione del sistema predisposto e delle norme sulla protezione dei dati personali, il Titolare, unitamente al DPO, predispone l'adozione di ulteriori misure correttive. Qualora, in sede di verifiche periodiche, si riscontri la possibilità di migliorare ulteriormente il trattamento dei dati effettuati nei vari Uffici, nell'ottica dell'accountability, il Titolare, unitamente ai Responsabili dei Servizi ed al DPO, procederà al riesame ed alla sostituzione delle misure già applicate.

TITOLO V – DIRITTI DEGLI INTERESSATI

Art. 19. Obbligo di informativa

19.1 Prima che si inizi qualunque trattamento di dati personali, il Titolare del trattamento fornisce all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti.

19.2 L'atto di informazione deve essere reso:

- in caso di dati personali raccolti presso l'interessato, prima dell'inizio del trattamento, al momento della raccolta dei dati, ai sensi dell'art. 13 GDPR;

- in caso di dati non ottenuti presso l'interessato, ai sensi dell'art. 14 GDPR:

  - entro un termine ragionevole, e comunque entro un mese dal loro ottenimento;
  - nel caso in cui i dati siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;
  - nel caso in cui sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Non è necessario fornire l'informativa se:

- l’interessato dispone già di tutte le informazioni necessarie;
- la comunicazione di tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell’interessato, anche rendendo pubbliche le informazioni;
- l’ottenimento o la comunicazione sono espressamente previsti dalla legislazione, nel rispetto delle misure appropriate per tutelare gli interessi legittimi dell’interessato;
- in presenza di un obbligo di legge che imponga la riservatezza e segretezza dei dati personali.

Art. 20. Contenuto dell’atto di informazione

20.1 L’atto di informazione deve essere fornito per iscritto o con altri mezzi, in formato cartaceo o elettronico, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Se richiesto dall’interessato, le informazioni possono essere rese anche oralmente, previa verifica dell’identità dell’interessato.

20.2 L’atto di informazione deve presentare il seguente contenuto:

- indicazione del Comune, quale Titolare del trattamento, ed i dati di contatto;

- i dati di contatto del DPO;

- indicazione delle finalità e della base giuridica del trattamento;

- il legittimo interesse perseguito dal Titolare o dal terzo, qualora questo costituisca la base giuridica del trattamento;

- gli eventuali destinatari dei dati personali;

- l’eventuale intenzione del Titolare di trasferire i dati personali a un Paese extra UE o ad un’organizzazione internazionale;

- il periodo di conservazione dei dati personali o il criterio utilizzato per determinare tale periodo;

- l’indicazione dei diritti esercitabili dall’interessato: diritto di accesso, rettifica, cancellazione, limitazione, opposizione e reclamo al Garante;

- qualora il trattamento si basi sul consenso, l’esistenza del diritto di revocare il consenso in qualsiasi momento;

- le modalità di trattamento, compresa l’esistenza di un eventuale processo decisionale automatizzato, compresa la profilazione;

- se la comunicazione dei dati è un obbligo legale o contrattuale o un requisito necessario per la conclusione del contratto e le possibili conseguenze della mancata comunicazione dei dati.

Nel caso di atto di informazione ai sensi dell'art. 14 GDPR, l'informativa conterrà anche l'indicazione delle categorie di dati trattati e la fonte da cui hanno origine i dati trattati e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

Art. 21. Informativa relativa ai sistemi di videosorveglianza

21.1 Il Comune ha adottato un sistema di videosorveglianza comunale. Gli interessati devono essere informati che stanno per accedere in una zona videosorvegliata, anche in caso di eventi e in occasione di pubblici spettacoli. A tal fine, il Comune ha adottato il modello di informativa semplificata predisposto dal Garante. L'atto di informazione completo è disponibile sul sito del Comune e presso i locali del Comune.

21.2 Il supporto con l'informativa semplificata:

- deve essere collocato prima del raggio di azione delle telecamere, anche nelle loro immediate vicinanze e non necessariamente in contatto con gli impianti;

-deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;

- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Art. 22. Consenso dell'interessato

22.1 La base giuridica dei trattamenti posti in essere dal Comune è data dalla necessità di eseguire compiti di interesse pubblico, anche rilevante, o connesso a pubblici poteri. Per questo motivo, il consenso al trattamento dei dati non è richiesto, a meno che il Comune non agisca per specifiche finalità diverse da quelle istituzionali.

22.2 Qualora sia necessario acquisire il consenso dell'interessato, la richiesta di consenso deve essere chiara, semplice, comprensibile e facilmente accessibile. Il Titolare deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.

22.3 Il consenso può essere revocato in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basato sulla revoca prima del consenso.

Art. 23. Diritto di accesso ai dati

23.1 Ai sensi dell'art. 15 GDPR, l'interessato ha diritto di ottenere dal Titolare del trattamento la conferma o meno che sia in corso un trattamento di dati personali che lo riguardano, ed in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari e le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica (art. 16 GDPR) o la cancellazione dei dati personali (art. 17) o la limitazione del trattamento dei dati personali che lo riguardano (art. 18) o di opporsi al loro trattamento (art. 21), nei casi previsti dalla normativa;

f) il diritto di proporre reclamo ad un'autorità di controllo, anche avvalendosi di un organismo, un'organizzazione o un'associazione senza scopo di lucro ai sensi dell'art. 80 GDPR;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

23.2 La richiesta va inoltrata in forma scritta dall'interessato senza particolari formalità: nel caso in cui sia inoltrata con mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato. La richiesta può essere inoltrata al Titolare, ai designati al trattamento indicati nell'atto di informazione o al DPO.

23.3 Il Titolare del trattamento deve fornire risposta entro un mese dal ricevimento della richiesta; tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità della questione. In tal caso, il Titolare deve avvisare l'interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta.

23.4 Le informazioni fornite sono gratuite. In caso di richieste manifestamente infondate o eccessive, in particolare per il carattere ripetitivo delle stesse, il Titolare può addebitare un contributo spese ragionevole, tenuto conto dei costi amministrativi sostenuti o rifiutare di soddisfare la richiesta.

Art. 24. Diritto alla rettifica

24.1 L'interessato ha diritto di ottenere, previa richiesta scritta, la rettifica da parte del Comune dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo. L'interessato ha altresì diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa. Il Titolare deve comunicare ai destinatari cui sono stati trasmessi i dati l'avvenuta rettifica, salvo che ciò risulti impossibile o implichi uno sforzo sproporzionato.

24.2 Il Titolare deve fornire risposta entro un mese dal ricevimento della richiesta; tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità della questione. In tal caso, il Titolare deve avvisare l'interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta

Art. 25. Diritto alla cancellazione – diritto all'oblio

25.1 L'interessato ha diritto di ottenere dal Titolare, previa richiesta scritta, la cancellazione dei dati che lo riguardano, senza ingiustificato ritardo nei seguenti casi:

- se i dati non sono più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati;

- l'interessato ha revocato il consenso al trattamento;

- l'interessato si è opposto al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;

- i dati personali sono stati trattati illecitamente;

- i dati personali devono essere cancellati per adempiere ad un obbligo legale previsto dalla legge.

Nei casi in cui i dati trattati siano stati diffusi pubblicamente sul web, il Titolare, tenuto conto dei costi di attuazione, è tenuto ad informare altri titolari che trattino i medesimi dati della richiesta di cancellazione di qualsiasi link, copia o riproduzione.

25.2 Il Titolare deve fornire risposta entro un mese dal ricevimento della richiesta; tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità della questione. In tal caso, il Titolare deve avvisare l'interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta

25.3 Il diritto alla cancellazione non trova applicazione se il trattamento è necessario:

a) per l'adempimento di un obbligo legale del Titolare o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri;

b) ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, qualora la richiesta di cancellazione rischi di rendere impossibile o pregiudicare gravemente il conseguimento degli obiettivi;

c) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

25.4 Il Titolare deve comunicare ai destinatari cui sono stati trasmessi i dati l'avvenuta cancellazione, salvo che ciò risulti impossibile o implichi uno sforzo sproporzionato.

Art. 26. Diritto di limitazione

26.1 L'interessato, previsa richiesta scritta, ha diritto di ottenere la limitazione del trattamento:

- nel caso in cui contesti l'esattezza dei dati personali, per il periodo necessario alla verifica da parte del Comune;
- in caso di trattamento illecito, se si oppone alla cancellazione dei dati chiedendo che invece ne sia limitato l'utilizzo;
- in caso di esercizio del diritto di opposizione, nell'attesa di verificare i presupposti del relativo diritto.

26.2 Il Titolare deve fornire risposta entro un mese dal ricevimento della richiesta; tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità della questione. In tal caso, il Titolare deve avvisare l'interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta

26.3 Se il trattamento è limitato, tali dati possono essere trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.

26.4 L'interessato che ha ottenuto la limitazione del trattamento è informato dal titolare del trattamento prima che detta limitazione sia revocata. Il Titolare deve comunicare ai destinatari cui sono stati trasmessi i dati l'avvenuta limitazione, salvo che ciò risulti impossibile o implichi uno sforzo sproporzionato.

Art. 27. Diritto di opposizione

27.1 L'interessato ha diritto di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione.

27.2 Tale diritto può essere esercitato salvo che sussistano motivi legittimi cogenti per procedere al trattamento che prevalgano sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

27.3 Il Titolare deve fornire risposta entro un mese dal ricevimento della richiesta; tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità della questione. In tal caso, il Titolare deve avvisare l'interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta

Art. 28. Diritto alla portabilità

28.1 Il diritto alla portabilità di cui all'art. 20 GDPR non può trovare applicazione in quanto il trattamento dei dati da parte del Comune è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

TITOLO VI – MEZZI DI TUTELA E RESPONSABILITA'

Art. 29. Soggetti responsabili e tutela giurisdizionale

29.1 Il Comune, quale titolare del trattamento, è responsabile del danno materiale o immateriale causato da una violazione del GDPR, ed è tenuto a risarcire il soggetto danneggiato, salvo che dimostri che l'evento dannoso non gli è in alcun modo imputabile.

29.2 I responsabili del trattamento rispondono dei danni causati dal trattamento solo se non hanno adempiuto gli obblighi del GDPR specificamente diretti ai responsabili, o hanno agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. Qualora sussista la responsabilità sia del Titolare che del Responsabile del trattamento, ciascuno risponde in solido verso il danneggiato.

29.3 L'azione risarcitoria va proposta avanti all'autorità giudiziaria ordinaria secondo le disposizioni di legge in materia.

Art. 30. Reclamo all'Autorità Garante

30.1 In alternativa al ricorso avanti all'autorità giudiziaria, l'interessato che ritenga di aver subito una violazione dei dati personali può proporre reclamo al Garante, ai sensi degli articoli 141 e seguenti del Codice Privacy.

TITOLO VII – VARIE

Art. 31. Abrogazioni

31.1 Il presente Regolamento sostituisce ogni precedente regolamento in materia di trattamento dei dati personali adottato prima dell'entrata in vigore del GDPR.

Art. 32. Entrata in vigore del Regolamento

32.1 Il presente Regolamento entra in vigore il giorno in cui diviene esecutiva la relativa delibera di approvazione.

32.2 Il Regolamento verrà pubblicato sul sito internet del Comune, nella sezione Amministrazione Trasparente. Una copia del Regolamento verrà consegnata al Segretario Comunale, ai dipendenti e ai collaboratori del Comune.

Art. 33. Norme applicabili

33.1. Per tutto quanto non espressamente disciplinato con il presente Regolamento, si applicano le disposizioni del GDPR e del Codice Privacy.