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

Sommario

Art. 1-Oggetto del Regolamento

1) Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del General Data Protection Regulation del 27 aprile 2016 n. 679, Regolamento Generale Protezione Dati (di seguito indicato come "GDPR"), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati.

Art. 2-Titolare del trattamento

1) Il Comune di Lagnasco è il Titolare del trattamento (di seguito indicato anche con "Titolare" o "Comune") dei dati personali trattati nell'ambito della propria organizzazione e struttura.
2) Al Titolare sono riconducibili le seguenti principali competenze e obblighi:
   a) Determinare le finalità e i mezzi del trattamento dei dati personali (art. 4 del GDPR);
   b) Agevolare l'esercizio dei diritti dell'interessato (art. 12 del GDPR) e fornire agli interessati le informazioni indicate dal GDPR (artt. 13 e 14 del GDPR);
   c) Mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento;
   d) Individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28 del GDPR);
   e) Tenere un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30 del GDPR);
   f) Garantire l'idonea formazione del personale incaricato del trattamento (art. 32 del GDPR);
   g) Comunicare all'Autorità di controllo (art. 33 del GDPR) e agli interessati (art. 34 del GDPR) eventuali violazioni dei dati;
   h) 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, effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 del GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 10 del presente Regolamento.
   i) Designare il responsabile della protezione dei dati (art. 37 del GDPR), mettendolo in grado di svolgere adeguatamente la propria attività (art. 38 del GDPR).
3) Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del GDPR: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.
4) Il Titolare 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 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 e per agevolare l'esercizio dei diritti dell'interessato, stabiliti dagli articoli 15-22 del GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
5) 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.
6) Le competenze sopra elencate e le altre previste nel GDPR sono attribuite agli organi del Comune in relazione alle funzioni agli stessi assegnati dalla Legge n. 56/2014, dal D.lgs. n. 267/2000 e dallo statuto comunale. In particolare:
   a) Al Consiglio Comunale sono assegnate eventuali competenze di tipo regolatorio o programmatorio generale in materia di protezione dei dati;
   b) All'organo esecutivo (Giunta comunale) sono assegnate tutte le competenze a carattere non gestionale e non rientranti nella competenza del Consiglio, con particolare riferimento agli atti e attività a contenuto organizzativo e di indirizzo;
   c) All'organo di vertice (Sindaco) competono le nomine, con riferimento in particolare ai soggetti designati del trattamento e al responsabile della protezione dei dati;
   d) Ai Responsabili del servizio, in qualità di facenti funzione del Titolare del trattamento, secondo l'ambito di competenza, spettano i seguenti compiti:
      i) Verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;

ii) Disporre, in conseguenza alla verifica di cui alla lett. i), le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
iii) Adottare soluzioni di privacy by design e by default;
iv) Contribuire al costante aggiornamento del registro delle attività di trattamento;
v) Garantire la corretta informazione e l'esercizio dei diritti degli interessati;
vi) Individuare i soggetti designati a compiere operazioni di trattamento (di seguito anche "designati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento e, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
vii) Disporre l'adozione dei provvedimenti imposti dal Garante Privacy;
viii) Collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
ix) Adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri Responsabili di servizio, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;
x) Individuare negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali i soggetti che effettuano tali trattamenti quali designati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
xi) Garantire al DPO e all'amministratore di sistema (se nominato) i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
xii) Effettuare la preventiva valutazione d'impatto (DPIA) ai sensi dell'art. 35 del GDPR, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
xiii) Consultare il Garante Privacy, in aderenza all'art. 36 del GDPR, nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'art. 35 indichi che il trattamento presenta un rischio residuale elevato;
xiv) Individuare i responsabili esterni del trattamento fornendo le necessarie indicazioni.

7) In assistenza al Titolare del trattamento è costituito un gruppo di gestione delle attività di trattamento composto dal segretario generale del Comune, dal Responsabile per la transizione digitale e dal Responsabile della prevenzione della corruzione e della trasparenza. Al gruppo compete il coordinamento generale delle funzioni e attività in materia di trattamento dati con particolare riferimento alla gestione delle relazioni con il DPO, all'organizzazione della formazione rivolta al personale, alla proposta di aggiornamento della modulistica, alla formulazione di istruzioni in materia di trattamento e verifica della loro applicazione.
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. 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. A titolo esemplificativo e non esaustivo, rientrano in questo ambito i trattamenti compiuti per:
      i) L'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
      ii) La gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
      iii) L'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione;
   b) L'adempimento di un obbligo legale al quale è soggetto il Comune;

c) L'esecuzione di un contratto con soggetti interessati;
d) 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) Sono nominati Responsabili esterni del trattamento di dati personali i soggetti estranei all'amministrazione comunale che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del Titolare.
2) Qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.
3) Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono contenere quanto previsto dall'art. 28, p. 3, del GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante Privacy oppure dalla Commissione europea.
4) Il Titolare del trattamento definisce di volta in volta se autorizzare la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

Art. 5-Contitolari del trattamento

1) Nel caso di esercizio associato di funzioni e servizi, allorché il Comune determini insieme a uno o più Titolari le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del GDPR.
2) I Titolari del trattamento determinano in modo trasparente, mediante accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR. Il contenuto essenziale dell'accordo è messo a disposizione degli interessati, mediante pubblicazione, per la durata del trattamento, sul sito web del Titolari del trattamento.
3) 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 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

Art. 6-Designati al trattamento

1) Per tutti i compiti non svolti in quanto Titolare, ogni Responsabile del servizio è individuato quale designato al trattamento dei dati personali relativamente ai servizi e uffici di competenza, in forza dell'incarico dirigenziale, mediante designazione scritta.
2) I dipendenti, assunti a qualsiasi titolo presso il Comune, sono designati al trattamento dei dati personali in forza del contratto di lavoro e dell'inserimento nella struttura organizzativa del Comune, mediante designazione scritta.
3) I collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare sono designati al trattamento dati personali mediante designazione scritta nel contratto di incarico o allegata ad esso.
4) La designazione scritta deve contenere le istruzioni generali per il trattamento di dati personali.

Art. 7-Responsabile della protezione dati

1) Il Responsabile della protezione dei dati (in seguito indicato con "DPO") viene nominato dal Comune, che lo individua tra i propri dipendenti oppure tra i soggetti esterni dotati di competenza adeguata, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati.

2) Il DPO è incaricato dei seguenti compiti:
   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 del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
   b) Sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare.
   c) Sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;
   d) Fornire, se richiesto, un parere in merito alla 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 Privacy e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del DPO è comunicato dal Titolare del trattamento al Garante Privacy;
   f) Fornire supporto nella tenuta dei registri di cui al successivo art. 9;
   g) Svolgere altri compiti e funzioni a condizione che il Titolare del trattamento si assicuri che non diano adito a un conflitto di interessi. In via esemplificativa, tali compiti e funzioni possono consistere in attività di supporto per verifica e attuazione disposizioni normative in materia di amministrazione trasparente, pubblicazioni social e siti web, con particolare riferimento agli aspetti di tutela dei dati personali. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.
3) Il Titolare del trattamento assicura che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   a) Il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/responsabili, che abbiano per oggetto questioni inerenti la protezione dei dati personali;
   b) 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;
   c) 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;
   d) Il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.
4) Nello svolgimento dei compiti affidatigli, il DPO 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 DPO:
   a) Procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
   b) Definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare del trattamento.
5) Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio del Comune.
6) La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
   a) Il ruolo di Responsabile per la prevenzione della corruzione e per la trasparenza;
   b) Qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
7) Il Titolare del trattamento fornisce al DPO le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali e ai trattamenti. In particolare è assicurato al DPO:

a) Supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti di settore e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;
b) Tempo sufficiente per l'espletamento dei compiti affidati al DPO;
c) Supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero tramite la costituzione di una Unità Operativa, ufficio o gruppo di lavoro DPO (formato dal DPO stesso e dal rispettivo personale);
d) Comunicazione ufficiale della sua nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno del Comune;
e) Accesso garantito ai settori funzionali del Comune così da garantire allo stesso il supporto, le informazioni e gli input essenziali per lo svolgimento dei propri compiti.

8) Il DPO 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.
9) Il DPO non può essere rimosso o penalizzato dal Titolare e per l'adempimento dei propri compiti.
10) Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare. 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.

Art. 8-Sicurezza del trattamento

1) Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2) Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono tra le altre, se del caso: 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 la sicurezza del trattamento.
3) Costituiscono misure tecniche ed organizzative che possono essere adottate dal Titolare del trattamento:
   a) Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
   b) Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici;
   c) Altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
4) Il Comune si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per proprio conto ed abbia accesso a dati personali.

Art. 9-Registri dei trattamenti

1) Il Titolare del trattamento predispone e tiene il Registro delle attività di trattamento svolte sotto la propria responsabilità e il Registro di tutte le categorie di attività relative al trattamento svolte per conto di un altro Titolare del trattamento.
2) Il Registro delle attività del Titolare del trattamento reca almeno le seguenti informazioni:
   a) Il nome ed i dati di contatto del Comune e del DPO;
   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 o 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.

3) I Registri dei trattamenti sono conservati dal Titolare del trattamento presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative del Comune.
4) Il Titolare del trattamento può farsi coadiuvare dal DPO nel compito di tenere i Registri, sotto la responsabilità del medesimo Titolare.

Art. 10-Valutazioni d'impatto sulla protezione dei dati (DPIA)

1) Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una DPIA ai sensi dell'art. 35 del GDPR, considerando la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2) Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, del GDPR e delle Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.
3) La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, del 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 del 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.
4) 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 tale trattamento non possa 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.
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. Il Dirigente di settore deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. L'Amministratore di sistema, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

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. L'Amministratore di sistema, se nominato, 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.
7) La DPIA non è necessaria nei casi seguenti:
   a) Se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, del GDPR;
   b) 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;
   c) 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;
   d) 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.
8) Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante Privacy e che proseguano con le stesse modalità oggetto di tale verifica.
9) 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:
      i) Delle finalità specifiche, esplicite e legittime;
      ii) Della liceità del trattamento;
      iii) Dei dati adeguati, pertinenti e limitati a quanto necessario;
      iv) Del periodo limitato di conservazione;
      v) Delle informazioni fornite agli interessati;
      vi) Del diritto di accesso e portabilità dei dati;
      vii) Del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
      viii) Dei rapporti con i responsabili del trattamento;
      ix) Delle garanzie per i trasferimenti internazionali di dati.
   c) Consultazione preventiva del Garante privacy;
   d) 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;
   e) 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.
10) 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.
11) Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento in caso le risultanze della DPIA condotta indichino l'esistenza di un rischio residuale elevato.
12) 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. 11-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 di titolarità del Comune.
2) Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore dalla scoperta del fatto e comunque senza ingiustificato ritardo.
3) I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:
   a) Danni fisici, materiali o immateriali alle persone fisiche;
   b) Perdita del controllo dei dati personali;
   c) Limitazione dei diritti, discriminazione;
   d) Furto o usurpazione d’identità;
   e) Perdite finanziarie, danno economico o sociale;
   f) Decifratura non autorizzata della pseudonimizzazione;
   g) Pregiudizio alla reputazione;
   h) Perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
4) Se il Titolare 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 verificatasi. I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione, a titolo di esempio, può:
   a) Coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   b) Riguardare categorie particolari di dati personali;
   c) Comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
   d) 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);
   e) Impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
5) La notifica deve prevedere il contenuto minimo richiesto dall’art. 33 del GDPR, ed anche la comunicazione all’interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
6) Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. 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 GDPR.

Art. 12-Rinvio

1) Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del GDPR e tutte le sue norme attuative vigenti.
2) Si mantengono inoltre in vigore, fino all’attuazione con modalità diverse, quanto già disciplinato da precedenti atti e regolamenti in merito ai sistemi di videosorveglianza.

ALLEGATI

A) Registro delle attività di trattamento

GLOSSARIO REGOLAMENTO

Ai fini della proposta di Regolamento comunale, si intende per:

Titolare del trattamento

Il Comune che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.

Responsabile del trattamento

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

Designato al trattamento

Il lavoratore della struttura organizzativa del Comune, che viene autorizzato dal Titolare del trattamento all'esecuzione di specifiche attività di trattamento per conto del Titolare stesso.

Responsabile per la protezione dati – DPO

Soggetto interno o esterno alla struttura organizzativa del Comune, che nominato dallo stesso svolge i compiti previsti dall'art. 39 del GDPR.

Registri delle attività di trattamento

Elenchi dei trattamenti, svolti dal Comune in qualità di Titolare o Responsabile del trattamento, tenuti in forma cartacea o informatizzata.

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

Procedura finalizzata a descrivere il trattamento, determinarne necessità e proporzionalità e facilitare la valutazione e gestione dei rischi per i diritti e le libertà delle persone fisiche connesse al trattamento dei loro dati personali.

Garante Privacy

Autorità Garante per la protezione dei dati personali istituita dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente.

GLOSSARIO REGISTRI

Ai fini delle proposte dei registri, si intende per:

Finalità del trattamento:	Specifico scopo perseguito dal Titolare nell'effettuare il trattamento di dati.
Base giuridica del trattamento:	Condizione di liceità applicabile alla specifica finalità perseguita e in particolare: Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; Adempimento di un obbligo legale al quale è soggetto il Comune; Esecuzione di un contratto con i soggetti interessati o di misure precontrattuali adottate su richiesta degli interessati; Consenso dell'interessato.
Operazioni di 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.
Modalità di trattamento:	Specifica se il trattamento avviene attraverso modalità cartacee e/o digitali.
Contitolare:	Specifica se il trattamento è svolto da due Titolari del trattamento che ne determinano congiuntamente finalità e mezzi.
Responsabile esterno:	Specifica se il trattamento è svolto in tutto o in parte da un soggetto esterno all'organizzazione del Titolare per conto dello stesso.
Dati art. 9 GDPR:	Specifica se il trattamento in esame coinvolge che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona.
Dati art. 10 GDPR:	Specifica se il trattamento in esame coinvolge dati relativi a condanne penali o reati o a connesse misure di sicurezza.
Termine ultimo di conservazione:	Arco di tempo in cui avviene il trattamento dei dati, che corrisponde al conseguimento delle finalità per i quali i dati sono trattati.
Interessati:	Soggetti a cui i dati personali oggetto di trattamento si riferiscono.
Interessati minori di 18 anni:	Specifica se tra gli interessati sono presenti minori di 18 anni.
Destinatari:	Soggetti esterni all'organizzazione del Titolare a cui vengono comunicati o messi a disposizione i dati oggetto di trattamento.

Trasferimento extra UE:	Specifica se i dati oggetto di trattamento sono trasferiti fuori dal territorio dell'Unione europea.
Valore rischio potenziale lordo	Livello di rischio valutato in base a probabilità di accadimento e dimensioni possibili del danno o gravità dell'evento per i diritti e le libertà degli interessati, senza tenere in considerazione controlli e misure di sicurezza adottate dal Titolare del trattamento.
Misure di sicurezza adottate:	Misure tecniche e organizzative adottate per mitigare il rischio.
Valore rischio effettivo netto	Livello di rischio mitigato dalle contromisure di sicurezza applicate.