COMUNE DI CALCIO

Provincia di Bergamo

REGOLAMENTO
PER LA GESTIONE
DELLA RISERVATEZZA
DEI DATI PERSONALI

Approvato con deliberazione del Consiglio Comunale nr. 15 del 06/05/2022

GLOSSARIO

RGPD = Regolamento Generale sulla Protezione dei Dati Personali, Regolamento UE n. 679/2016 (in inglese GDPR General Data Protection Regulation)

RPD = Responsabile della Protezione dei dati (in inglese DPO Data Protection Officer)

Data breach = "riuscire a fare breccia", qualunque violazione dei dati personali

DPIA = Valutazione di impatto sulla protezione dei dati

Privacy by design = Privacy dal momento della sua progettazione. Implica che qualsiasi progetto va realizzato assumendo dalla fase iniziale di ideazione misure di protezione di dati personali

Privacy by default = protezione dei dati per impostazione predefinita, ovvero, misure tecniche ed organizzative che assicurano solo i dati personali necessari per ogni specifica finalità di trattamento

Audit Privacy = è una valutazione dei processi interni adottati sul grado di rispetto della normativa vigente del Reg. UE n. 679/2016

GEPD = Garante Europeo della protezione dei dati

Accountability = letteralmente "rendere conto", ovvero, il Titolare del trattamento si deve responsabilizzare autonomamente nella gestione ed organizzazione della Privacy. Il principio nasce nella legislazione europea e statunitense ed è inteso come la responsabilità dell'amministrazione verso chi l'ha scelta e si fonda su: trasparenza, intesa come informazioni dell'attività di governo; partecipazione di chiunque al miglioramento delle politiche pubbliche; collaborazione, intesa come efficacia dell'azione amministrativa attraverso la cooperazione tra tutti i livelli di governo

WP 29 = Gruppo di lavoro Art. 29, organismo consultivo ed indipendente, composto da un rappresentante dei Garanti dei dati personali di ogni stato membro, da un rappresentante della Commissione UE e dal Garante europeo della protezione dei dati

INDICE

GLOSSARIO 1
TITOLO I - PRINCIPI 4
Art. 1 - Finalità 4
Art. 2 - Principi del trattamento 4
Art. 3 - Definizioni 5
TITOLO II - SOGGETTI DEL TRATTAMENTO DEI DATI 6
Art. 4 - Titolare del trattamento 6
Art. 5 - Responsabili del trattamento 6
Art. 6 - Competenze del Responsabile della protezione dei dati (DPO) 7
Art. 7 - Responsabili esterni di trattamento 8
TITOLO III - TRATTAMENTO DEI DATI PERSONALI 10
Art. 8 - Trattamento dati particolari 10
Art. 9 - Principi del trattamento dei dati particolari e giudiziari 10
Art. 10 - Individuazione di interesse pubblico rilevante 11
Art. 11 - Pubblicazione web per obblighi di trasparenza 12
Art. 12 - Pertinenza delle informazioni contenenti dati personali 13
Art. 13 - Trattamento dei dati personali effettuato con sistemi di videosorveglianza 13
Art. 14 - Registro del trattamento 14
TITOLO IV - DIRITTI DELL'INTERESSATO 14
Art. 15 - Diritto di accesso ed alla portabilità dei dati 14
Art. 16 - Diritto di limitazione 15
Art. 17 - Diritto all'oblio 15
Art. 18 - Diritto alla rettifica dei dati 16
Art. 19 - Diritto di opposizione 16
Art. 20 - Obbligo di informativa 16
Art. 21 - Contenuto dell'informativa 17
Art. 22 - Informativa per utilizzo di sistemi di videosorveglianza 18
Art. 23 - Consenso 18
TITOLO V - MISURE DI SICUREZZA 18
Art. 24 - Misure di sicurezza preventive 18
Art. 25 - D.P.I.A. 19
Art. 26 - Procedimento 20
Art. 27 - Consultazione preventiva del Garante della privacy 20
Art. 28 - Misure di sicurezza minime per trattamenti con strumenti elettronici ed informatici 21
Art. 29 - Misure per trattamenti non automatizzati 21

Art. 30 - Misure per dati raccolti con sistemi di videosorveglianza 22
Art. 31 - Sistema e politica di audit 23
Art. 32 - Procedimento di audit 23
Art. 33 - Monitoraggio 23
TITOLO VI - DATA BREACH O VIOLAZIONE DEI DATI PERSONALI 24
Art. 34 - Definizione di violazione dati personali 24
Art. 35 - Procedimento in caso di data breach 25
Art. 36 - Notifica al Garante della privacy 25
Art. 37 - Comunicazione all'interessato 26
Art. 38 - Documentazione della violazione - Registro della violazione 26
TITOLO VII - MEZZI DI TUTELE E RESPONSABILITÀ 27
Art. 39 - Soggetti responsabili ed azione risarcitoria 27
Art. 40 - Reclamo 27
Art. 41 - Trattamento illecito dei dati 27
Art. 42 - Falsità nelle dichiarazioni e notificazioni al Garante della privacy 28
Art. 43 - Omessa predisposizione di misure di sicurezza 28
TITOLO VIII - ENTRATA IN VIGORE 28
Art. 44 - Abrogazioni 28
Art. 45 - Entrata in vigore del regolamento 28

TITOLO I - PRINCIPI

Art. 1 - Finalità

1. Il presente regolamento disciplina le misure organizzative ed i processi interni di attuazione del Regolamento UE n. 679/2016 (RGPD o GDPR) ai fini del trattamento di dati personali per finalità istituzionali nel Comune di CALCIO (di seguito "Comune").

2. Ai fini del presente regolamento, per funzioni istituzionali si intendono quelle:

a) previste dalla legge, dallo statuto comunale e dai regolamenti;
b) esercitate in attuazione di convenzioni, accordi, nonché sulla base degli strumenti di programmazione e pianificazione previsti dalla legislazione vigente;
c) svolte per l'esercizio dell'autonomia organizzativa, amministrativa e finanziaria dell'ente locale;
d) in esecuzione di un contratto con i soggetti interessati;
e) per finalità specifiche e diverse dai punti precedenti, purché l'interessato esprima il consenso al trattamento.

3. Il presente regolamento è conforme alle norme e principi costituzionali, nonché alle altre disposizioni vigenti in materia di privacy.

Art. 2 - Principi del trattamento

1. Per le finalità indicate al precedente art. 1, il Comune effettua il trattamento dei dati personali nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, nonché del diritto alla riservatezza ed all'identità di persone fisiche e giuridiche.

2. In attuazione del comma 1, i dati personali sono:

- trattati in conformità delle norme di legge, cioè in modo lecito e con trasparenza nei confronti dell'interessato;
- corretti, esatti ed aggiornati a seguito di intervenute variazioni;
- solo quelli necessari e pertinenti allo scopo specifico, con la riduzione al minimo delle informazioni identificative; il trattamento va evitato laddove lo scopo specifico può essere raggiunto tramite dati anonimi;
- trattati con adeguate misure di sicurezza, in modo da evitare abusi, o illeciti, o perdita, o distruzione o danno accidentale, in conformità al principio di integrità e riservatezza.

3. Relativamente al trattamento di dati personali di persone decedute, il diritto alla riservatezza si estingue con la morte del titolare. I diritti di cui al Titolo IV del presente regolamento, in tale caso, possono essere esercitati da chi agisce per la tutela del defunto, o per motivi familiari meritevoli di tutela.[1]

[1] *Il Reg. UE n. 679/2016 non si applica alle persone decedute, ma lascia liberi gli Stati membri di provvedere ed in merito il riferimento per la nostra legislazione è l'art. 9, co. 3, del D.Lgs. n. 196/2003, da considerarsi ancora vigente. Per la giurisprudenza del Consiglio di Stato sopravvive una forma di tutela dei dati sensibili – come altre forme di tutela – anche dopo la morte, ma nelle forme specifiche e diverse previste dal citato art. 9, co. 3, per la tutela del defunto e per ragioni familiari meritevoli di protezione. (cfr. Consiglio di Stato, Sez. III, sentenza 12 giugno 2012, n. 3459).*

Art. 3 - Definizioni

Ai fini del presente regolamento si adottano le seguenti definizioni:

- Dati personali: qualunque informazione riguardante una persona fisica identificata o identificabile;
- Trattamento: qualsiasi operazione compiuta con o senza processi automatizzati, che prevede la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'utilizzo, la trasmissione, la diffusione o altra forma di messa a disposizione di dati personali;
- Profilazione: trattamento automatizzato di dati personali per valutare determinati aspetti personali relativi ad una persona fisica, come, a titolo esemplificativo, rendimento professionale, situazione economica;
- Archivio: insieme strutturato di dati personali accessibili secondo criteri determinati;
- Pseudonimizzazione: trattamento di dati in modo che non si possa risalire all'identificazione dell'interessato senza informazioni aggiuntive, conservate separatamente e soggette a misure di sicurezza;
- Titolare del trattamento: ente locale che, anche congiuntamente, determina e decide le finalità ed i mezzi del trattamento;
- Responsabile del trattamento: persona fisica o giuridica o ente pubblico che tratta i dati per conto del Titolare del trattamento;
- Destinatario: persona fisica, o giuridica, o ente pubblico che riceve comunicazione di dati personali;
- Terzo: chiunque (persona fisica, giuridica, ente pubblico) diverso dall'interessato, dal titolare del trattamento, dal responsabile del trattamento e da ogni incaricato;
- Consenso dell'interessato: ogni manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con cui viene manifestato il suo assenso e viene conferita legittimità al trattamento dei propri dati personali;
- Violazione dei dati personali: ogni diffusione, trasmissione, accesso, comunicazione non autorizzata;
- Dati relativi alla salute: dati personali sensibili sullo stato di salute fisica e mentale di una persona fisica, inclusa la prestazione di servizi di assistenza sanitaria, inclusi i dati genetici e biometrici;
- Dati giudiziari: i dati personali relativi alle condanne penali e ai reati, o a connesse misure di sicurezza.

TITOLO II - SOGGETTI DEL TRATTAMENTO DEI DATI

Art. 4 - Titolare del trattamento

1. Il Titolare del trattamento dei dati personali è il Comune, rappresentato, ai fini legali previsti dal Regolamento UE n. 679/2016, dal Sindaco pro-tempore. Esso è il Responsabile per tutte le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati e può agire tramite un suo delegato[2] per le competenze attribuite dal presente regolamento.
2. Il Comune adotta tutte le misure tecniche ed organizzative idonee a garantire che il trattamento sia conforme ai principi di cui all'art. 2 del presente regolamento e ciò deve essere dimostrabile.
3. Tramite verifiche periodiche, deve vigilare sull'osservanza delle istruzioni scritte impartite ai Responsabili e sul pieno rispetto delle vigenti disposizioni in materia di trattamento dati.
4. 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, ogni Comune mantiene la titolarità dei propri dati e crea un accordo di nomina a Responsabile esterno ad ogni ente associato.

Art. 5 - Responsabili del trattamento

1. Il Titolare del trattamento dei dati nomina, con provvedimento motivato (Decreto Sindacale), il Responsabile della Protezione dei dati (DPO - Data Protection Officer), un supervisore indipendente, che deve essere obbligatoriamente designato dai soggetti apicali (il Sindaco per i Comuni) di tutte le pubbliche amministrazioni.
2. Le funzioni del DPO (contenute nell'articolo 39 del Regolamento UE 2016/679) riguardano, principalmente, la consulenza, al titolare e ad eventuali responsabili del trattamento, sul rispetto degli obblighi derivanti dal RGPD e dalla normativa nazionale, oltre che la verifica della relativa osservanza. Al DPO si chiede, inoltre, di cooperare con l'autorità di controllo e di esserne il punto di riferimento per facilitare l'accesso a documenti e informazioni riguardanti l'azienda o l'ente ed, in ultimo, di collaborare con titolare e responsabili di settore, se richiesto, alla valutazione di impatto sulla protezione dei dati e di sorvegliarne lo svolgimento.
3. I Responsabili di settore sono anch'essi nominati con un provvedimento Sindacale e provvederanno, a loro volta, a nominare e ad impartire istruzioni agli incaricati sottoposti, a seguito di un confronto con il DPO in carica.
4. Il nominativo e le modalità di contatto del DPO vanno pubblicati nel sito del Comune nella sezione Amministrazione Trasparente.
5. Il DPO è incaricato almeno dei seguenti compiti:
   - informare e fornire consulenza al titolare del trattamento, o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal presente regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

[2] *Il Garante privacy ha chiarito, già nel parere 11 dicembre 1997, che il Titolare del trattamento, per un ente locale, è il Comune nel suo complesso, rappresentato dal Sindaco. Il Comune, tuttavia, agisce, di volta in volta, con i suoi Responsabili. Il Segretario comunale non è il Titolare del trattamento, ma può essere nominato Responsabile unico del trattamento.*

- sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del titolare del trattamento, o del responsabile del trattamento, in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del RGPD, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti, il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Art. 6 - Competenze del Responsabile della protezione dei dati (DPO)

1. Il Responsabile della protezione dei dati (D.P.O. - Data Protection Officer) va tempestivamente informato di tutte le questioni riguardanti la protezione dei dati personali e, nell'eseguire i propri compiti, considera i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. In particolare:

- informa e fornisce consulenza al Titolare del trattamento o al Responsabile di settore, nonché agli altri dipendenti[3];
- verifica l'applicazione corretta della disciplina sul trattamento dei dati personali, ferma restando la responsabilità del Titolare e del Responsabile di trattamento; sorveglia le attribuzioni di responsabilità, le attività di formazione e controllo effettuate dal Titolare e dal Responsabile del trattamento;
- fornisce, ai sensi dell'art. 25 del presente regolamento, il parere sulla necessità di procedere alla valutazione di impatto sulla protezione dei dati personali;
- collabora in sede di audit nella mappatura dei processi e nella individuazione delle non conformità, per le quali suggerisce misure correttive. Successivamente, sovrintende i monitoraggi periodici delle soluzioni adottate, per verificare la necessità di eventuali riesami o sostituzione delle misure, ai sensi degli artt. 31-33 del presente regolamento;
- funge da tramite con il Garante per la consultazione preventiva, ai sensi dell'art. 27 del presente regolamento, in caso residuino rischi elevati in un trattamento, dopo l'adozione della valutazione di impatto sulla protezione dei dati personali;
- fornisce parere al Titolare del trattamento in caso di violazione dei dati personali per la valutazione della gravità del data breach.

[3] *Sebbene il Regolamento non utilizzi il termine di incaricato (art. 30 Codice privacy – D.Lgs. 30 giugno 2003, n. 196), di fatto è riscontrabile nelle persone autorizzate al trattamento dei dati (art. 28, par. 3, lett. b) oppure art. 4, par. 1, punto 10) del RGPD). Nel Comune è da intendersi incaricato ogni dipendente che, per le proprie mansioni, è autorizzato con atto scritto a trattare dati personali.*

2. Il DPO esprime parere non vincolante; l'eventuale adozione di condotta difforme da quella da lui suggerita va motivata.
3. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; non deve ricevere istruzioni in merito al loro svolgimento, né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il DPO non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

Art. 7 - Responsabili esterni di trattamento

1. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati, in qualità di responsabili del trattamento, stipulando atti giuridici in forma scritta, che specifichino la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto, o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che indichi la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto, o altro atto giuridico, prevede, in particolare, che il responsabile del trattamento:

- tratti i dati personali secondo il regolamento in materia di privacy in vigore, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure richieste ai sensi dell'articolo 32 del RGPD;
- rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
- tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo IV;

- assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
- metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento, o da un altro soggetto da questi incaricato. Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi, in materia di protezione dei dati, contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva, nei confronti del titolare del trattamento, l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato (art. 40 RGPD) o a un meccanismo di certificazione approvato (art. 42 RGPD) può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui al paragrafo 4 del presente articolo.

6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto, o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo, può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43 del RGPD.

7. La Commissione UE può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2, del RGPD.

8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63 del RGPD.

9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo è stipulato in forma scritta, anche in formato elettronico.

10. Fatti salvi gli articoli 82, 83 e 84 del RGPD, se un responsabile del trattamento viola il presente regolamento determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

TITOLO III - TRATTAMENTO DEI DATI PERSONALI

Art. 8 - Trattamento dati particolari[4]

1. Gli uffici del Comune trattano i dati particolari, sensibili ai sensi dell'art. 9 del RGPD, che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, biometrici, relativi alla salute, alla vita sessuale ed i dati giudiziari:

- per motivi di interesse pubblico rilevante come specificati nel successivo art. 10;
- per un interesse vitale dell'interessato o di altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- se l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche;
- per diritti dell'interessato in materia di diritto del lavoro e sicurezza sociale e protezione sociale autorizzato da norma di legge o contratto collettivo;
- se il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- se il trattamento è necessario ai fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici ed è proporzionato alla finalità perseguita.

2. In tutti i casi indicati vanno sempre previste misure di garanzia appropriate e specifiche per tutelare i diritti fondamentali e gli interessati. A tal fine, si applicano le misure di sicurezza previste nel Titolo V del presente regolamento.

3. I dati particolari riguardanti lo stato di salute non devono essere divulgati.

Art. 9 - Principi del trattamento dei dati particolari e giudiziari

1. I dati particolari di cui all'articolo precedente sono trattati sempre nel rispetto dei principi indicati nell'art. 2, ovvero devono essere esatti, pertinenti, non eccedenti ed indispensabili rispetto alle finalità perseguite e sono aggiornati periodicamente.

2. I raffronti e le interconnessioni con altre informazioni sensibili e giudiziarie detenute dal Comune sono consentite soltanto previa verifica della loro stretta indispensabilità nei singoli casi ed indicazione scritta dei motivi che ne giustificano l'effettuazione. Lo stesso vale se le predette operazioni sono effettuate utilizzando banche di dati di diversi titolari del trattamento, nonché per la diffusione di dati sensibili e giudiziari, che sono ammesse esclusivamente previa verifica della loro stretta indispensabilità nei singoli casi e nel rispetto dei limiti e con le modalità stabiliti dalle disposizioni legislative che li prevedono.

3. Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali.

4. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o dello Stato che preveda garanzie appropriate per i diritti e le libertà degli interessati.

[4] Gli artt. 8-10 del presente regolamento assorbono il regolamento dei dati sensibili e giudiziari (non più come regolamento separato quindi) e sono stati redatti tenendo presente il provvedimento generale del Garante privacy del 30 giugno 2005 e lo schema tipo predisposto dall'Anci. L'art. 9 del RGPD rinomina la categoria dei dati sensibili come particolare e specifica meglio i casi in cui possono essere trattati.

Art. 10 - Individuazione di interesse pubblico rilevante

I trattamenti di interesse pubblico rilevante effettuati dal Comune sono i seguenti:

STATO CIVILE, ANAGRAFE E LISTE ELETTORALI

Sono considerati di rilevante interesse pubblico i trattamenti dei dati relativi alla tenuta degli atti e dei registri dello stato civile, dell'anagrafe sia dei residenti in Italia che degli italiani all'estero, nonché delle liste elettorali.

CITTADINANZA, IMMIGRAZIONE E CONDIZIONE DELLO STRANIERO

Sono considerati di rilevante interesse pubblico i trattamenti dei dati e le attività dirette all'applicazione della disciplina in materia di cittadinanza, di immigrazione, di asilo, di condizione dello straniero e di profugo e dello stato di rifugiato. In particolare, è ammesso il trattamento dei dati strettamente necessari per l'adozione di talune tipologie di atti e provvedimenti (rilascio di visti, permessi, attestazioni, autorizzazioni e documenti anche sanitari).

ESERCIZIO DEI DIRITTI POLITICI E PUBBLICITÀ DELL'ATTIVITÀ DI DETERMINATI ORGANI

Sono considerate di rilevante interesse pubblico le attività finalizzate all'applicazione della disciplina in materia di elettorato attivo e passivo e di esercizio di altri diritti politici, nonché dirette all'esercizio del mandato degli organi rappresentativi. Sono, altresì, rilevanti le attività finalizzate all'applicazione della disciplina relativa alla documentazione dell'attività istituzionale degli organi pubblici.

RAPPORTI DI LAVORO

Sono considerate di rilevante interesse pubblico le attività finalizzate all'instaurazione ed alla gestione dei rapporti di lavoro, sia in ordine all'espletamento degli adempimenti previsti in relazione al trattamento economico e giuridico, sia in materia sindacale che di igiene e sicurezza del lavoro.

MATERIA TRIBUTARIA

Sono considerate di rilevante interesse pubblico le attività dirette all'applicazione, anche tramite i concessionari del servizio, delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti e ai Responsabili d'imposta, nonché in materia di deduzioni e detrazioni.

BENEFICI ECONOMICI ED ABILITAZIONI

Sono considerate di rilevante interesse pubblico le attività finalizzate all'applicazione della disciplina in materia di benefici economici, agevolazioni, elargizioni, altri emolumenti ed abilitazioni. Tra questi sono espressamente ricompresi i trattamenti necessari alle comunicazioni, alle certificazioni ed alle informazioni previste dalla normativa antimafia, quelli relativi all'applicazione in materia di usura ed antiracket, nonché quelli necessari al rilascio di licenze e autorizzazioni.

VOLONTARIATO E SERVIZI SOCIALI

Sono considerate di rilevante interesse pubblico le attività finalizzate all'applicazione della disciplina in materia di rapporti con le organizzazioni di volontariato, nella specie per quanto concerne l'erogazione di contributi, nonché:

- interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;
- interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;
- assistenza nei confronti di minori, anche in relazione a vicende giudiziarie.

ATTIVITÀ DI PREDISPOSIZIONE DI ELEMENTI DI TUTELA IN SEDE AMMINISTRATIVA O GIURISDIZIONALE

Sono di rilevante interesse pubblico i trattamenti di dati effettuati in conformità di leggi o di regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi.

RAPPORTI CON ENTI DI CULTO

Sono considerati di rilevante interesse pubblico i trattamenti strettamente necessari allo svolgimento dei rapporti istituzionali con gli enti di culto, con le confessioni e le comunità religiose.

Art. 11 - Pubblicazione web per obblighi di trasparenza

1. Il Comune effettua il trattamento di dati personali contenuti in atti e documenti amministrativi, che devono essere pubblicati sul web per obblighi di trasparenza previsti dal D.Lgs. n.33/2013.
2. I documenti di cui al comma 1 sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione e vanno mantenuti aggiornati.
3. Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.
4. I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati particolari relativi alla vita sessuale non possono essere diffusi per finalità di trasparenza.
5. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.
6. I dati vanno pubblicati in formato di tipo aperto ai sensi dell'art. 68 del D.Lgs. n. 82/2005 e sono liberamente riutilizzabili secondo la normativa vigente. I dati personali diversi dai dati sensibili e dai dati giudiziari possono essere diffusi attraverso siti istituzionali, nonché trattati secondo modalità che ne consentano la indicizzazione e la rintracciabilità tramite i motori di ricerca web.
7. I dati, le informazioni e i documenti di cui al comma 1 sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione.
8. Deroghe alla predetta durata temporale quinquennale sono previste:
   a) nel caso in cui gli atti producano ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;

b) per 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, regionale e locale, ai sensi dell'art. 14, comma 2, del D.Lgs. n. 33/2013 e i titolari di incarichi dirigenziali e di collaborazione o consulenza che devono rimanere pubblicati online per i tre anni successivi alla cessazione del mandato o dell'incarico, ai sensi dell'art. 15, comma 4, del D.Lgs. n. 33/2013;
c) nel caso in cui siano previsti diversi termini dalla normativa in materia di trattamento dei dati personali.

9. I dati personali devono essere conservati, in ogni caso, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati; l'interessato ha sempre diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.

Art. 12 - Pertinenza delle informazioni contenenti dati personali

1. Non possono essere disposti filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione Trasparente".
2. Qualora i dati personali contenuti nei documenti non siano pertinenti o siano eccedenti rispetto all'interesse manifestato dal richiedente nell'istanza di ostensione, al fine di salvaguardare la riservatezza di terzi, l'accesso agli atti può essere limitato, su valutazione del Responsabile del procedimento, mediante l'occultamento di alcuni contenuti.

Art. 13 - Trattamento dei dati personali effettuato con sistemi di videosorveglianza

1. Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza richiede apposita informativa agli interessati e questa può essere rilasciata in forma semplificata come indicato all'art. 22 del presente regolamento.
2. Per finalità di tutela della sicurezza urbana, la durata della conservazione dei dati è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione, in conformità dell'art. 6, comma 8, del D.L. n. 11/2009. Tempi di durata maggiore della conservazione dei dati necessitano di richiesta al Garante adeguatamente motivata, con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti (es. collaborazione con l'autorità giudiziaria o con la polizia giudiziaria in relazione ad un'attività investigativa in corso).
3. Ai dati raccolti mediante sistemi di videosorveglianza vanno applicate misure di sicurezza adeguate, ai sensi dell'art. 30 del presente regolamento.

Art. 14 - Registro del trattamento

1. Il Titolare del trattamento istituisce e tiene aggiornato, in forma scritta ed in formato elettronico, coadiuvato dal DPO e dai Responsabili di settore designati, un registro delle attività di trattamento svolte sotto la propria responsabilità.
2. Il Registro privacy del Titolare del trattamento deve contenere almeno le seguenti informazioni:
   - estremi identificativi e di contatto del Comune;
   - estremi identificativi e di contatto Responsabile della protezione dei dati;
   - finalità del trattamento;
   - descrizione delle categorie di interessati;
   - descrizione delle categorie di dati personali;
   - categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   - eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale con documentazione delle garanzie in materia di privacy;
   - termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   - descrizione generale delle misure di sicurezza tecniche e organizzative adottate.
3. In caso di richiesta del Garante, il Registro privacy è messo immediatamente a disposizione.

TITOLO IV - DIRITTI DELL'INTERESSATO

Art. 15 - Diritto di accesso ed alla portabilità dei dati

1. L'interessato ha sempre diritto di ottenere dal Titolare del trattamento la conferma che sia in corso un trattamento dei dati personali che lo riguardano, di averne accesso e di acquisire le seguenti informazioni:
   - finalità del trattamento;
   - categoria di dati trattati;
   - i destinatari a cui i dati personali sono comunicati;
   - il periodo di conservazione dei dati previsto o, se non è possibile, i criteri utilizzati per determinare tale periodo;
   - l'esistenza del proprio diritto a richiedere la rettifica o cancellazione del dato o la limitazione dei dati o di opporsi al loro trattamento;
   - l'esistenza di un processo automatizzato e della profilazione dei dati, nonché informazioni sulla logica utilizzata.
2. La richiesta va inoltrata, in forma scritta, dall'interessato, senza particolari formalità; in caso sia inoltrata con mezzi elettronici, salvo contraria indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.
3. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità, ma, in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
4. I Responsabili del trattamento di settore sono tenuti a collaborare per la verifica della sussistenza del diritto, chiedendo informazioni all'interessato e, se necessarie, anche al fine di identificarlo e,

successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole. In tale ipotesi, va rilasciata copia del documento richiesto.
5. Il rilascio della copia è gratuito; in caso di richiesta di copie ulteriori il rilascio può essere subordinato al pagamento di un contributo per costi amministrativi.
6. Il diritto alla portabilità dei dati di cui all'articolo 20 del RGPD non si applica ai trattamenti svolti dal Comune necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso ente.

Art. 16 - Diritto di limitazione

1. L'interessato, previa richiesta scritta, ha diritto ad ottenere la limitazione del trattamento:
- in caso sia contestata 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, invece, che ne sia limitato l'utilizzo;
- in caso di esercizio di opposizione nell'attesa della verifica dei presupposti del relativo diritto.

2. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità, ma, in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
3. I Responsabili di settore sono tenuti a collaborare per la verifica della sussistenza del diritto, chiedendo informazioni all'interessato e, se necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.
4. In caso di riscontro favorevole, va comunicato all'interessato che ha ottenuto la limitazione del trattamento, senza ritardo e prima che la limitazione sia revocata nei casi 1 e 3 (del comma 1). Vanno, altresì, avvisati i destinatari della limitazione dei dati, a meno che ciò sia impossibile o richieda uno sforzo sproporzionato.

Art. 17 - Diritto all'oblio

1. L'interessato ha diritto a chiedere al Titolare del trattamento, con richiesta scritta, la cancellazione dei dati personali che lo riguardano:
- se non sono più necessari per le finalità per le quali sono stati raccolti o trattati;
- se si oppone al trattamento e non sussiste motivo legittimo prevalente per procedere al trattamento;
- se i dati sono illecitamente trattati.

2. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolare complessità, ma, in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
3. I Responsabili di settore sono tenuti a collaborare per la verifica della sussistenza del diritto, chiedendo informazioni all'interessato e, se necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.

4. Nel caso in cui i dati siano stati diffusi pubblicamente anche su siti web, il Titolare del trattamento, tenendo conto dei costi di attuazione, è tenuto ad informare altri titolari che trattano i medesimi dati della richiesta di cancellazione di qualsiasi link, copia o riproduzione.
5. Nel caso in cui i dati non siano diffusi pubblicamente e su siti web, il Titolare del trattamento è tenuto ad avvisare i destinatari della cancellazione dei dati, a meno che ciò sia impossibile o richieda uno sforzo sproporzionato.

Art. 18 - Diritto alla rettifica dei dati

1. L'interessato ha diritto a chiedere, con richiesta scritta, la rettifica da parte del Comune, senza ingiustificato ritardo, dei dati personali inesatti che lo riguardano. La rettifica include anche la possibile integrazione dei dati avuto riguardo alla finalità del trattamento.
2. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolare complessità, ma, in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
3. I Responsabili di settore sono tenuti a collaborare per la verifica della sussistenza del diritto, chiedendo informazioni all'interessato e, se necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.

Art. 19 - Diritto di opposizione

1. L'interessato può presentare per iscritto richiesta di opposizione al trattamento dei dati personali che lo riguardano per motivi connessi alla sua situazione particolare, inclusa la profilazione.
2. Il Titolare del trattamento entro trenta giorni fornisce risposta all'interessato a seguito della valutazione della situazione: è consentito l'esercizio del diritto se non esistano comprovati motivi basati su norma di legge per procedere al trattamento prevalenti sugli interessi del richiedente, o se si tratta di esercizio o accertamento di un diritto in sede giudiziaria.
3. Il termine di cui al precedente comma può essere prorogato di due mesi in casi di particolare complessità, ma, in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
4. I Responsabili di settore sono tenuti a collaborare nel procedimento interno di verifica dei presupposti del diritto di opposizione.
5. In ogni comunicazione all'interessato deve essere inserito l'avviso, in modo chiaro e separato dal restante contenuto dell'atto, che questi può esercitare il diritto all'opposizione.

Art. 20 - Obbligo di informativa[5]

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

[5] Il REGOLAMENTO UE 679/2016, in realtà usa, al posto di informativa, il termine informazioni, per dare l'idea di una pluralità di atti informativi che possono avvenire nell'arco dell'intero trattamento dei dati; un adempimento dinamico reso effettivo per l'attività del Titolare del trattamento e del destinatario. Il documento, però, può essere ancora denominato Informativa, fermo restando la conformità dei suoi contenuti ai nuovi articoli 13 e 14 del Reg. UE.

2. L'informativa privacy deve essere fornita per iscritto, in formato cartaceo o elettronico, o, qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.
3. Essa va effettuata:
- in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, nel momento della raccolta dei dati;
- in caso di dati personali non ottenuti presso l'interessato: 1) entro un termine ragionevole, massimo di un mese dalla raccolta (non dalla registrazione) dei dati; 2) nel caso in cui i dati vadano comunicati all'interessato alla prima comunicazione; 3) se i dati personali devono essere comunicati ad un altro destinatario, non oltre la prima comunicazione.

4. Non è necessario fornire l'informativa:
- nel caso in cui l'interessato disponga già di tutte le informazioni necessarie;
- nel caso in cui la comunicazione risulti impossibile o implicherebbe uno sforzo sproporzionato; in particolare, per il trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica;
- a fini statistici. In tali casi, il Titolare del trattamento adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con pubbliche informazioni;
- in presenza di un obbligo di legge che impone la riservatezza e segretezza dei dati personali.

Art. 21 - Contenuto dell'informativa

1. L'informativa è gratuita e deve essere sintetica, presentare un linguaggio chiaro e semplice ed essere, in ogni caso, comprensibile per l'interessato.
2. Essa presenta il seguente contenuto:
- indicazione del Comune Titolare del trattamento e del Responsabile del trattamento;
- indicazione del Responsabile della protezione dei dati;
- indicazione di ogni finalità istituzionale di trattamento e della norma giuridica di riferimento;
- indicazione di finalità aventi fondamento in contratto o in richiesta dell'interessato;
- indicazione delle modalità di trattamento distinte anche in base all'ufficio del Comune che lo effettua, evidenziando se sia un trattamento automatizzato (con eventuale possibilità di profilazione e della sua logica) o se sia un trattamento cartaceo;
- indicazione dei destinatari;
- il periodo di conservazione dei dati personali e, se non è previsto da norma di legge, il criterio utilizzato dal Titolare per la durata del trattamento;
- l'indicazione dei diritti che l'interessato può esercitare, ovvero: accesso, integrazione e rettifica, eventuale revoca, portabilità, oblio, opposizione e reclamo;
- le conseguenze in caso di rifiuto del trattamento o di omessa comunicazione di dati.

3. Il Titolare del trattamento può, di volta in volta, aggiungere ogni ulteriore informazione che si ritiene necessaria al caso concreto.

Art. 22 - Informativa per utilizzo di sistemi di videosorveglianza

1. Nel caso di utilizzo di sistemi di videosorveglianza per finalità di sicurezza urbana, gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).
2. A tal fine, può essere utilizzato un modello di informativa semplificata, che, poi, rinvii a un testo contenente tutti gli elementi completi di cui all'articolo precedente, disponibile agevolmente senza oneri per gli interessati, sia sul sito internet dell'amministrazione comunale, che nella sede della polizia municipale.
3. In ogni caso, il Titolare, anche per il tramite di un incaricato, ove richiesto, è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'articolo precedente.
4. Il supporto con l'informativa:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a 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. 23 - Consenso

1. Il consenso al trattamento dei dati non è richiesto dal Comune in quanto pubblica amministrazione se agisce per finalità istituzionali.
2. Il consenso può essere richiesto se il Comune agisce per specifiche finalità diverse da quelle istituzionali, ai sensi dell'art. 1, comma 1, lett. e), del presente regolamento. In tal caso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.
3. La richiesta di consenso deve essere comprensibile, facilmente accessibile, chiara e semplice.
4. Il consenso può essere revocato ed, in tal caso, la revoca non pregiudica la liceità del trattamento già effettuato.

TITOLO V - MISURE DI SICUREZZA[6]

Art. 24 - Misure di sicurezza preventive

1. Il Comune deve adottare misure che soddisfino la protezione dei dati fin dalla progettazione e della protezione dei dati di default; ovvero, mette in atto misure tecniche ed organizzative adeguate sia prima del trattamento, sia nell'atto del trattamento stesso[7], come indicate nel presente titolo.

[6] Il presente titolo del regolamento è stato redatto tenendo conto, oltre che delle norme del Reg. UE n. 679/2016, delle Linee guida in materia di D.P.I.A. del Gruppo Art.29 aggiornate il 4/10/2017, delle norme e degli allegati del D.Lgs. n. 196/2003 ancora vigenti, delle raccomandazioni del Garante del 29 novembre 2000 per i dati personali trattati con sistemi di videosorveglianza, delle norme standard BS 10012:2017, nonché delle norme sulla sicurezza ISO/IEC27040.

[7] Il comma dell'articolo proposto, in particolare, e tutto il titolo delle misure di sicurezza, in generale, tiene conto del Considerando 78, in cui viene esplicitato quanto elaborato in dottrina, in relazione ad un sistema privacy by design e by default. Per privacy by design si intende un sistema che prima del trattamento dei dati adotti misure per incrementare la sicurezza, quali le tecniche di anonimizzazione e pseudonimizzazione. Per privacy by default

2. Il Comune, in particolare:

- utilizza le tecniche di pseudonimizzazione dei dati personali;
- tratta i soli dati necessari per ogni specifica finalità, al fine di garantire la massima protezione dei dati attraverso il loro minimo trattamento;
- custodisce e controlla i dati personali in modo da ridurre al minimo, mediante l'adozione di misure di sicurezza preventive, i rischi di distruzione, perdita, anche accidentale, de dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità pubbliche di raccolta;
- provvede a formare il personale sugli obblighi in materia di protezione dei dati personali, in relazione alle specifiche competenze rivestite dai singoli dipendenti e dai rispettivi uffici in cui sono inseriti.

3. 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 RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 25 - D.P.I.A.

1. Oltre alle misure preventive di cui all'articolo precedente, il Comune quando un trattamento presenta, a seguito di analisi, rischi elevati per i diritti e le libertà degli interessati, procede alla valutazione di impatto sulla protezione dei dati (D.P.I.A.).

2. La D.P.I.A. può riguardare una singola operazione di trattamento o due o più trattamenti simili, che presentano rischi elevati analoghi.

3. Ricorrono rischi elevati, ai sensi dell'art. 35, par. 3, lett. a)-c) del Reg. UE 679/2016, in presenza di:

- una valutazione sistematica di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulle quali si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su tali persone fisiche;
- trattamento su larga scala, di categorie particolari di dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, relativi alla salute, alla vita sessuale o a condanne penali, a reati e a misure di sicurezza;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. In caso ricorra uno dei tre indici di cui al comma precedente, il Comune deve procedere nella D.P.I.A.

5. Il Comune, altresì, redige una valutazione di impatto del rischio se ricorrono due dei seguenti indici forniti dal Garante:

- valutazione o assegnazione di un punteggio inclusiva di profilazione, in particolare in considerazione di 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;

---

si intende un'applicazione del principio di minimizzazione dell'uso dei dati personali; ovvero, vanno trattati i soli dati necessari per ogni specifica finalità; massima protezione dei dati attraverso il loro minimo trattamento.

- dati sensibili o di carattere altamente personale;
- trattamento di dati su larga scala;
- creazione di corrispondenze o combinazione di insiemi di dati;
- dati relativi a interessati vulnerabili considerato lo squilibrio di potere tra gli interessati ed il Comune;
- uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

6. Il Titolare, se lo ritiene opportuno, può procedere anche alla D.P.I.A. in caso ricorra anche uno solo dei requisiti sopra indicati e può individuare anche altri criteri di riscontro del rischio elevato in base alla specifica circostanza.

Art. 26 – Procedimento

1. Qualora ricorra un rischio elevato, il Titolare del trattamento chiede il parere del Responsabile della Protezione dei dati (DPO) e, se lo ritiene opportuno, degli stessi interessati.
2. La D.P.I.A. deve presentare il seguente contenuto minimo:
- una descrizione dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi.

3. La D.P.I.A. può essere effettuata anche da un Responsabile del trattamento, ma la responsabilità finale è del Titolare del trattamento.
4. Nel caso in cui la D.P.I.A. non riesca a trattare in maniera sufficiente i rischi individuati, per quelli residui va effettuata, tramite il Responsabile della protezione dei dati, la consultazione del Garante.

Art. 27 - Consultazione preventiva del Garante della privacy

1. Nei casi in cui si è proceduto nella valutazione di impatto sulla protezione dei dati ed è emerso che il Comune non riesce a trattare in maniera sufficiente tutti i rischi elevati, poiché ne restano ancora alcuni, per questi ultimi residui va consultato preventivamente il Garante per la privacy.
2. Il Comune, tramite il Responsabile della protezione dei dati (DPO), ai sensi degli artt. 36 e 39, par. 1, lett. e), del Regolamento UE n. 679/2016, invia richiesta di consultazione al Garante, comunicando:
- i dati dell'ente locale, in quanto Titolare del trattamento, ed i propri dati in quanto punto di contatto e referente per la consultazione;
- le finalità ed i mezzi di trattamento previsti;
- le misure di garanzia previste per proteggere i diritti e le libertà fondamentali degli interessati;
- la valutazione di impatto sulla protezione dei dati in versione completa;
- ogni altra informazione ritenuta necessaria.

3. Il Garante formula parere scritto entro otto settimane dal ricevimento della richiesta di consultazione, nel caso in cui ritenga che il trattamento comunicato violi le norme sulla protezione dei dati e, in particolare, qualora ritenga che il Comune non abbia sufficientemente attenuato o

identificato il rischio. In base alla complessità del trattamento previsto, il Garante può prorogare la sua risposta di un termine aggiuntivo di sei settimane, informando il Responsabile della protezione dei dati entro un mese dal ricevimento della richiesta di consultazione.
4. In caso sia necessario, il Garante può richiedere al Responsabile della protezione dei dati informazioni aggiuntive a quelle già comunicate e può sospendere la decorrenza dei termini di cui al comma 3 in attesa della loro trasmissione.
5. In assenza di parere espresso del Garante entro le otto settimane dal ricevimento della richiesta di consultazione, il Comune può procedere nel trattamento dei dati.

Art. 28 - Misure di sicurezza minime per trattamenti con strumenti elettronici ed informatici

1. Il Titolare del trattamento insieme al Responsabile della Protezione dei dati (DPO), vista la relazione annuale dell'Amministratore di sistema (AdS), in collaborazione con il Responsabile della Transizione Digitale (RTD), nel rispetto delle misure minime di sicurezza previste dall'Agenzia per l'Italia Digitale (AGID), misure compilate annualmente a carico dell'Ads, supervisiona il controllo delle banche dati organizzate in archivi elettronici, sentiti gli AdS Responsabili esterni del trattamento (i fornitori dei sistemi gestionali utilizzati) e verifica che siano state fornite, a tutto il personale che le utilizza, direttive per garantire che le operazioni informatiche di trattamento siano svolte senza rischi per gli interessati. In particolare, vengono adottate le seguenti misure di sicurezza:

- attribuzione agli incaricati di codici identificativi (parola chiave) composti da almeno otto caratteri, oppure, nel caso lo strumento elettronico non lo consenta, da un numero di caratteri pari al massimo consentito;
- modifica della parola chiave da parte dell'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi;
- disattivazione dei codici identificativi in caso di perdita della qualità degli stessi o di mancato utilizzo per un periodo superiore a sei mesi;
- protezione degli elaboratori contro i rischi di intrusioni, mediante l'utilizzo di appositi programmi;
- verifica dell'efficacia e dell'aggiornamento del software antivirus, almeno con cadenza semestrale;
- distruzione dei supporti di memorizzazione nel caso non siano riutilizzabili;
- applicazione di tecniche di pseudonimizzazione ai dati personali trattati;
- sistemi antiintrusioni e di protezione (firewall, antivirus, ecc.), misure antincendio;
- sistemi di copiatura e conservazione di archivi elettronici, misure idonee a ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico.

2. Sono, inoltre, impartite, con circolari interne, le istruzioni agli incaricati per non lasciare incustodito ed accessibile il proprio strumento elettronico durante una sessione di trattamento.

Art. 29 - Misure per trattamenti non automatizzati

1. Il Comune fornisce istruzioni scritte agli incaricati anche per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici, in particolare, per il controllo e la custodia, per l'intero ciclo

necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
2. I documenti che contengano dati sensibili e giudiziari sono controllati fino alla restituzione, in modo che non accedano ad essi persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate.
3. L'accesso agli archivi contenenti dati particolari è controllato.
4. 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. 30 - Misure per dati raccolti con sistemi di videosorveglianza

1. I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
2. Occorre rispettare i princìpi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo 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.
3. Devono, quindi, essere adottate almeno le seguenti specifiche misure tecniche ed organizzative:
- in presenza di differenti competenze 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 già menzionati soggetti, designati incaricati 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;
- laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere 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;
- nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle già menzionate 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;
- qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo.

4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, predisponendo apposita informativa di cui all'art. 22 del presente regolamento; inoltre, va determinato con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione ai sensi dell'art. 13 del presente regolamento.

Art. 31 - Sistema e politica di audit[8]

1. Il Comune mette in atto misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è conforme al Regolamento UE 679/2016 e, a tal fine, adotta il procedimento di audit in conformità anche delle politiche della qualità.
2. Il Comune, tramite il Responsabile della protezione dei dati, valuta, mediante audit, i processi interni all'ente locale per:

- verificare il grado di conformità del trattamento dei dati personali effettuato da tutti gli uffici alla normativa vigente;
- verificare che tutti i dipendenti osservino le regole per la liceità e la sicurezza del trattamento di dati personali;
- verificare l'efficacia di azioni correttive a seguito di "non conformità".

3. Il processo consiste:
– in una prima mappatura delle possibili situazioni di rischio che si verificano nel Comune in base alla sua organizzazione interna, agli uffici ed al trattamento dei dati di ciascuno;
– nell'individuare situazioni di non conformità del trattamento agli standard minimi di sicurezza~~;~~
– nell'attuare azioni correttive.

Art. 32 - Procedimento di audit

1. Il Comune con il Responsabile della protezione dei dati (DPO), anche avvalendosi di esperti, procede nell'audit concretamente mediante:

- Incontro tra tecnici informatici, al fine di analizzare il sistema amministrativo informatico del Comune rispetto al nuovo regolamento europeo RGPD;
- Verifica delle pratiche di gestione privacy in relazione al nuovo regolamento europeo RGPD.

2. A seguito dell'attività di cui al comma precedente, vengono analizzati i risultati emersi che possono consistere in:

- situazioni di conformità;
- raccomandazioni per il miglioramento (istruzioni e corso di formazione per Responsabili ed Incaricati Comunali);
- situazioni di non conformità;

3. Tali risultati vengono formalizzati in un rapporto di Audit che dà atto di tutte le fasi del procedimento svolto e fornisce al Comune l'indicazione delle eventuali azioni correttive da realizzare.

Art. 33 - Monitoraggio

1. Il Comune verifica che vengano applicate le procedure interne e le misure di sicurezza adottate in sede di audit e, precisamente, che:

- venga fatto un uso corretto di mezzi informatici ai fini del trattamento dei dati personali, in particolare, monitorando l'utilizzo delle password e gli accessi agli archivi elettronici contenenti dati personali, con particolare attenzione ai dati sensibili;

[8] *Tale articolo rappresenta i contenuti minimi di ogni attività di auditing. Si rimanda alla Relazione per i dettagli.*

- venga fatto un corretto utilizzo degli archivi cartacei che conservano i dati personali, con particolare riguardo alla conservazione dei dati sensibili;
- vengano adeguatamente formati i dipendenti in modo diversificato in base alla modalità di trattamento cui sono preposti;
- ogni ufficio comunale tratti i dati secondo il principio di minimizzazione, ovvero, solo ciò che sia strettamente necessario, si accerti dell'esattezza e correttezza dei dati e che conservi i dati nel rispetto dei termini indicati dalle norme, laddove presenti, o, in subordine per il tempo strettamente necessario al raggiungimento della finalità di trattamento;
- in caso di incidenti o violazioni come descritte al titolo successivo, siano applicate le misure correttive per porre riparo agli effetti negativi;
- che siano garantiti i diritti degli interessati e correttamente curate le istanze di accesso, cancellazione, limitazione del trattamento, rettifica, nonché siano verificate le istanze di opposizione, nonché i reclami eventualmente presentati al Garante;
- che vengano tenuti sempre aggiornati i contenuti delle informative e siano adattate alle esigenze dei differenti uffici e differenti trattamenti;
- che i documenti contenenti dati personali, presenti nel sito internet del Comune, con particolare riferimento alla pubblicazione all'albo pretorio ed alla sezione Amministrazione Trasparente, siano conformi ai tempi di pubblicazione previsti dall'art. 124 del D.Lgs. n. 267/2000 e dal D.Lgs. n. 33/2013;
- che, nelle ipotesi di utilizzo di sistemi di videosorveglianza, vengano rispettate le specifiche misure di sicurezza come indicate negli artt. 13, 22, 30 del presente regolamento.

2. In caso di riscontro di non corretta applicazione del sistema di audit predisposto e delle norme sul trattamento dei dati personali, il Responsabile di trattamento, insieme al Responsabile della Protezione dei dati, predispone l'adozione di misure nuove correttive.

3. Se in sede di monitoraggio, con la collaborazione del Responsabile della protezione dei dati, si riscontri la possibilità di migliorare ulteriormente il trattamento dei dati effettuato dai vari uffici comunali, nell'ottica di obiettivi di efficienza, il Responsabile del trattamento procede nel riesame e nella sostituzione delle misure già applicate.

TITOLO VI - DATA BREACH O VIOLAZIONE DEI DATI PERSONALI

Art. 34 - Definizione di violazione dati personali

1. La violazione dei dati personali è una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali.

2. Per ***distruzione non autorizzata*** è da intendersi un'azione che rende irreversibile il processo di ricostruzione del dato personale, determinando la sua esatta e totale eliminazione in rerum natura.

3. Per ***perdita*** è da intendersi la fuoriuscita del dato trattato ai fini di privacy dalla sfera del legittimo detentore, in modo del tutto incontrollato e non tracciato.

4. Per ***modifica non autorizzata*** è da intendersi una deficienza organizzativa o fatti illeciti che, incidendo sulla conformazione del dato, sono capaci di arrecare danni fisici e morali agli interessati (es. si pensi, nel mondo della sanità, a casi di sostituzioni errate di terapie).
5. Per ***rivelazione non autorizzata*** è da intendersi la comunicazione di un segreto professionale.
6. Per ***accesso non autorizzato*** è da intendersi l'illecita attività di terzi (hacker) capaci di sottrarre e disporre di dati di un sistema attaccato grazie a particolari tecniche elusive di protezione.
7. Per ***soggetto non autorizzato*** è da intendersi ogni persona diversa da quella competente nell'ente a possedere e trattare i dati.

Art. 35 - Procedimento in caso di data breach

1. I Responsabili di settore, nel caso in cui vengano a conoscenza della violazione, informano, senza ingiustificato, ritardo il Titolare del trattamento e richiedono immediato parere al Responsabile della protezione dei dati sulla gravità della violazione, ovvero:
   - se questa sia inoffensiva per le misure di sicurezza già presenti in questo ente;
   - se può comportare rischi per gli interessati al trattamento ed il grado dei rischi;
   - le misure di sicurezza eventualmente da adottare per porre rimedio alla violazione.
2. I Responsabili di settore relazionano immediatamente al Titolare del trattamento la violazione, indicando la categoria di dati violati ed allegano il parere del Responsabile della protezione dei dati (DPO), in cui viene indicato se le misure presenti nel Comune rendono la violazione inoffensiva o, se invece, vanno integrate.
3. Al Titolare del trattamento compete la valutazione finale sulla gravità o meno della violazione. Nel caso in cui venga riscontrata la presenza di rischi per le persone fisiche, effettua, via Pec, la notifica del data breach al Garante per la privacy, entro 72 ore dal momento in cui ne è venuto a conoscenza o, se in un momento successivo, nel provvedimento indica i motivi del ritardo. Per la suddetta pratica, il Titolare può avvalersi delle competenze del DPO designato.

Art. 36 - Notifica al Garante della privacy

1. La notifica al Garante non è necessaria se la violazione è inoffensiva, ossia in caso di assenza di rischio per interessati e persone fisiche e ciò si verifica se il Comune, nel momento in cui essa è avvenuta, aveva misure di sicurezza che hanno reso i dati inintelligibili perché, per esempio, anonimi o cifrati in modo sicuro, attraverso un algoritmo standardizzato, o mediante schemi di cifratura a chiave simmetrica.
2. Non ricorre l'intellegibilità se la violazione ha portato la distruzione o la perdita dei dati personali.
3. La notifica al Garante deve presentare il seguente contenuto minimo:
   - la natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   - il nome e i dati di contatto del Responsabile della protezione dei dati, o di altro punto di contatto presso cui ottenere più informazioni;
   - le probabili conseguenze della violazione dei dati personali;

- le misure adottate da parte del Comune, o di cui si propone l'adozione, per porre rimedio alla violazione dei dati personali.

A questo contenuto minimo, è possibile aggiungere ogni altra informazione che il Titolare ritiene necessaria.

4. Qualora non si sia in possesso delle informazioni di cui al comma 3, il Titolare procederà a comunicare, entro 72 ore, quelle di cui è a conoscenza e, successivamente, appena verrà in possesso dei dati mancanti, effettuerà una comunicazione integrativa senza ingiustificato ritardo.

5. Il Garante può indicare l'adozione di misure integrative a quelle già descritte nella notifica, oltre che fornire osservazioni per porre rimedio alla violazione e può anche imporre la comunicazione all'interessato di cui al successivo articolo, qualora non sia stata ritenuta necessaria dal Comune.

Art. 37 - Comunicazione all'interessato

1. Il Titolare del trattamento comunica all'interessato, senza ingiustificato ritardo, la violazione in presenza solo di rischio elevato per i diritti e le libertà delle persone fisiche. Quanto più attuale è il dato violato, tanto maggiore è la probabilità di rischio elevato, intendendosi per attualità il tempo trascorso dall'acquisizione del dato.

2. La comunicazione all'interessato va effettuata con un linguaggio semplice e chiaro e deve presentare anch'essa un contenuto minimo, rappresentato da:

- il nome e i dati di contatto del Responsabile della protezione dei dati, o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate da parte del Titolare del trattamento, o di cui si propone l'adozione, per porre rimedio alla violazione dei dati personali.

3. Qualora non ricorrano i presupposti per la notifica al Garante, come indicati nell'articolo precedente, non si procede nemmeno alla comunicazione all'interessato.

Questa, inoltre, non è necessaria se:

- i dati violati erano soggetti a misure di protezione tali da renderli incomprensibili, perché, per esempio, sottoposti a cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione ad personam richiederebbe sforzi sproporzionati per l'elevato numero di interessati. In tal caso, il Comune può procedere ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia (es. tramite web o giornale locale).

Art. 38 - Documentazione della violazione - Registro della violazione

1. Il Titolare del trattamento documenta ogni violazione dei dati personali, la procedura avviata internamente all'ente locale ed i provvedimenti per porvi rimedio. A tal fine, redige apposita scheda tecnica cui sono allegati la relazione del Responsabile del trattamento ed il parere del RPD.

2. Il Titolare del trattamento annota la violazione nel *Registro delle violazioni*, che contiene, tra le altre informazioni: l'ufficio dell'ente locale competente al trattamento dei dati violati, la descrizione

e la gravità del data breach, l'indicazione dei dispositivi cartacei o automatizzati coinvolti, la categoria dei dati violati e dei destinatari, le misure di sicurezza presenti ed applicate ai dati violati e le ulteriori eventuali misure adottate.
3. La documentazione è a disposizione di eventuali ispezioni e verifiche da parte del Garante privacy.

TITOLO VII - MEZZI DI TUTELE E RESPONSABILITÀ

Art. 39 - Soggetti responsabili ed azione risarcitoria

1. Il Comune è Responsabile per ogni danno materiale o immateriale causato da una violazione dei dati personali trattati ed è tenuto a risarcire l'interessato o la persona fisica o giuridica danneggiata.
2. All'obbligazione risarcitoria verso il danneggiato è tenuto anche il Responsabile di settore, se il danno è stato causato da un suo inadempimento nell'ambito dei compiti a cui è stato preposto.
3. Il Titolare del trattamento ed il Responsabile di settore vanno esenti da responsabilità se provano che l'evento dannoso non è loro imputabile.
4. L'azione risarcitoria va proposta dinanzi all'autorità giudiziaria ordinaria, secondo le norme dell'ordinamento interno.
5. Il Responsabile della Protezione dei dati (DPO) non risponde nei confronti dei danneggiati, ma solo nei confronti del Comune Titolare del trattamento ed in relazione alle specifiche competenze attribuite al momento del conferimento dell'incarico e con successivi accordi scritti.

Art. 40 - Reclamo

1. Fatta salva la tutela giurisdizionale, l'interessato può presentare reclamo al Garante, se ritiene che il Comune abbia violato la riservatezza dei propri dati.
2. Il reclamo è presentato, in forma scritta, senza particolari formalità, al Garante e contiene la documentazione utile per la valutazione, nonché le informazioni sul Comune e sul Responsabile di trattamento, oltre che dell'interessato.
3. Il Garante effettua un'istruttoria preliminare, nel corso della quale può richiedere informazioni al Comune ed all'esito del procedimento può imporre al Comune di adottare i provvedimenti necessari per rendere il trattamento dei dati conforme alla disciplina vigente.
4. Il Garante informa l'interessato dello stato o dell'esito del reclamo.

Art. 41 - Trattamento illecito dei dati[9]

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto, o di recare ad altri un danno, procede al trattamento di dati personali in violazione delle norme sulla

[9] *Il diritto comunitario (Trattato di Lisbona) non consente all'Unione Europea di disciplinare le fattispecie di reato da perseguire negli Stati membri. Il Considerando 149 del Reg. UE n. 679/2016 rimanda agli Stati membri l'adozione di disposizioni relative a sanzioni penali per le violazioni del regolamento europeo; si ricorda anche la clausola contenuta nell'art. 6, par. 3, dello stesso Reg. UE n. 679/2016, in base alla quale gli Stati membri possono disciplinare – tra l'altro – in merito alla liceità di trattamento. Sono, pertanto, pienamente vigenti le norme del Codice privacy, D.Lgs. n. 196/2003, che disciplinano fattispecie dei seguenti reati: art. 167 trattamento illecito di dati; art. 168 falsità nelle dichiarazioni e notificazione al Garante; art. 170 inosservanza dei provvedimenti del Garante, nonché la contravvenzione di cui all'art. 169, consistente nell'omessa predisposizione di misure di sicurezza*

protezione dei dati personali, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto, o di recare ad altri un danno, procede al trattamento di dati personali in violazione delle norme sulla materia, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni e la pena accessoria della pubblicazione della sentenza ai sensi degli artt. 167 e 172 del D.Lgs. n. 196/2003.

Art. 42 - Falsità nelle dichiarazioni e notificazioni al Garante della privacy

I Responsabili di settore o il Responsabile della protezione dei dati (DPO) che, in esecuzione delle rispettive competenze, procedono, per conto del Comune, con notificazioni, comunicazioni al Garante, qualora forniscano false dichiarazioni o attestazioni o producano documenti falsi, salvo che il fatto costituisca reato più grave, sono puniti con la reclusione da sei mesi a tre anni e la pena accessoria della pubblicazione della sentenza, ai sensi degli artt. 168 e 172 del D.Lgs. n. 196/2003.

Art. 43 - Omessa predisposizione di misure di sicurezza

Il Titolare del trattamento e le persone fisiche che agiscono per suo conto che non adottino le misure di sicurezza minime sono penalmente responsabili e sono puniti, con arresto fino a due anni, dalle autorità giudiziarie competenti, oltre che con la pena accessoria della pubblicazione della sentenza, ai sensi degli artt.169 e 172 del D.Lgs. n. 196/2003.

TITOLO VIII - ENTRATA IN VIGORE

Art. 44 - Abrogazioni

1. Il presente regolamento sostituisce ogni altro atto in materia adottato prima dell'entrata in vigore del Regolamento UE 679/2016; per quanto non previsto dal presente regolamento, si applicano direttamente le norme del predetto regolamento europeo.
2. Il presente regolamento fa riferimento alle sole norme del Codice della privacy tuttora vigenti.

Art. 45 - Entrata in vigore del regolamento

1. Il presente regolamento entra in vigore ai sensi dell'art. 66 dello Statuto comunale.
2. Il regolamento e la relativa modulistica per l'esercizio dei diritti sono resi pubblici mediante pubblicazione sul sito internet del Comune, nella Sezione Amministrazione Trasparente.
3. Il presente regolamento va inoltrato al Segretario comunale, ai responsabili di settore, al DPO e a ogni altro dipendente che tratta dati personali nel Comune.