COMUNE DI URBINO

(Provincia di Pesaro e Urbino)

REGOLAMENTO COMUNALE PER L'ATTUAZIONE

DEL REG. U.E. N. 679 DEL 2016 E DEL CODICE PRIVACY

RELATIVAMENTE ALLA PROTEZIONE DEI DATI PERSONALI

DELLE PERSONE FISICHE

APPROVATO

dal Consiglio Comunale con deliberazione n. 33 del 01/04/2019

INDICE

TITOLO I Oggetto e finalità del trattamento
Art. 1 – Oggetto del Regolamento
Art. 2 - Finalità e base giuridica dei trattamenti
Art. 3 – Informativa

TITOLO II - Soggetti
Art. 4 - Titolare del trattamento
Art. 5 - Responsabile esterno del trattamento
Art. 6 - Responsabile della Protezione dei Dati (RPD)
Art. 7 – Amministrazione del Sistema Informatico
Art. 8 - Designato al trattamento
Art. 9 – Incaricato del trattamento

TITOLO III – Attività del Titolare
Art. 10 - Registro delle attività di trattamento
Art. 11 – Sistemi di I.C.T . – Pubblicazione degli atti e Amministrazione trasparente
Art. 12 - Segnalazione dei comportamenti illeciti dei dipendenti all'interno del Comune
Art. 13 – Sistemi di controllo a distanza dei luoghi di lavoro e monitoraggio degli accessi, mediante dispositivi elettronici
Art. 14 – Sistemi di videosorveglianza del territorio
Art. 15 – Open Data
Art. 16 – Conservazione dei dati e dei documenti informatici

TITOLO IV – Sicurezza, valutazione d'impatto, diritti dell'interessato, accesso agli atti e norme applicabili
Art. 17 - Sicurezza del trattamento
Art. 18 - Valutazioni d'impatto sulla protezione dei dati
Art. 19 - Violazione dei dati personali
Art. 20 – Diritti dell'interessato
Art. 21 – Accesso ai documenti amministrativi e accesso civico
Art. 22 - Norme applicabili e conservazione degli effetti degli atti amministrativi

TITOLO I – Oggetto del regolamento e finalità del trattamento

Art. 1 – Oggetto del Regolamento

1. Il presente Regolamento ha per oggetto l'individuazione dei soggetti coinvolti a vario titolo nelle attività di trattamento, le loro precipue funzioni e le regole comportamentali e le misure fisiche, tecniche ed organizzative, atte all'ottenimento di una corretta attuazione del Regolamento europeo n. 679 del 2016 (General Data Protection Regulation), di seguito indicato con "GDPR", nonché del Codice Privacy (D.Lgs 196/2003 e s.m.i.), con riguardo ai trattamenti dei dati personali delle persone fisiche attuati dal Comune al fine di garantire i diritti e le libertà degli interessati (persone fisiche).

Art. 2 - Finalità e base giuridica dei trattamenti

1. Il trattamento è effettuato dal Comune per le seguenti finalità:

- l'esercizio delle funzioni amministrative proprie che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
- la erogazione dei servizi connessi all'esercizio delle funzioni amministrative o su domanda degli interessati;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale e/o regionale delegate al Comune in base alla vigente legislazione.

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina, che ne costituisce la base giuridica, ed in particolare ai sensi dell'art. 6, comma 1°, del GDPR, alle lettere:
b) l'esecuzione di un contratto con i soggetti interessati;
c) l'adempimento di un obbligo legale al quale è soggetto il Comune;
e) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
f) l'interesse legittimo del titolare.
Il trattamento dei dati particolari di cui all'art. 9, comma 1°, del GDPR, necessario per le specifiche finalità di cui ai precedenti punti, è lecito purché all'interessato sia stata fornita una puntuale informativa su tale categoria di dati, o si verta nelle casistiche di cui al comma 2°, alle lettere b) e g).

Art. 3 – Informativa

1. Ogni struttura del Comune ogniqualvolta provvede alla raccolta dei dati personali, deve informare l'interessato in forma concisa, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro. L'informativa deve contenere: il nominativo ed i dati di contatto del Titolare – il nominativo ed i dati di contatto del Responsabile della Protezione dei dati - le finalità e le modalità del trattamento cui sono destinati i dati richiesti - la base giuridica del trattamento –le categoria di dati personali trattati - i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili – l'eventuale trasferimento dei dati in paesi terzi extra UE - il periodo di conservazione dei dati – l'esistenza di un eventuale processo decisionale automatizzato - i diritti dell'interessato di cui agli artt. 15 – 22 del GDPR, nonché di proporre reclamo all'Autorità di controllo.
2. L'informativa deve essere – di regola - resa per iscritto; può essere resa oralmente, o anche mediante affissione negli Uffici in cui gli interessati si recano per conferire i dati o con appositi moduli pubblicati sulle pagine Web dei singoli Uffici.
3. Se i dati personali non sono raccolti presso l'interessato, l'informativa è data al medesimo all'atto della registrazione dei dati o non oltre la prima comunicazione, eccetto nei seguenti casi: a) quando i dati sono trattati in base ad un obbligo previsto dalla legge o da un regolamento; b) quando i dati sono trattati per far valere o difendere un diritto dell'ente in sede giudiziaria, sempre che siano trattati solo per tale finalità e per il periodo necessario al loro perseguimento; c) quando la

comunicazione dell'informativa all'interessato comporti un impiego di mezzi sproporzionato rispetto al diritto tutelato.

TITOLO II - Soggetti

Art. 4 - Titolare del trattamento

1. Il Titolare del trattamento dei dati personali è il Comune. L'ente è rappresentato ai fini previsti dal GDPR dal Sindaco pro-tempore ai sensi dell'art. 50 del T.U.E.L.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR.
4. Le suddette misure sono definite fin dalla fase di progettazione e sono 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 da 15 a 22 del GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
5. Gli interventi necessari per l'attuazione delle medesime misure sono considerati nell'ambito della programmazione operativa (Documento Unico di Programmazione - DUP), e le risorse necessarie sono allocate nel bilancio di previsione e nel Piano Esecutivo di Gestione (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. Il Titolare adotta misure appropriate per fornire all'interessato:
a) le informazioni indicate dall'art. 13 del GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
b) le informazioni indicate dall'art. 14 del GDPR, qualora i dati personali non stati ottenuti presso lo stesso interessato.
7. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 del RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 18.
8. Il Titolare, inoltre, provvede:
a) ad individuare i Responsabili del trattamento nelle persone dei soggetti pubblici o privati eventualmente affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.
b) nominare il Responsabile della Protezione dei Dati (RPD) di cui al successivo art. 5;
c) nominare quali Designati al trattamento i Dirigenti/Responsabili delle Aree/Servizi secondo la struttura organizzativa dell'ente individuata con apposita deliberazione della Giunta comunale;
d) provvede alla formazione periodica di tutti i dipendenti autorizzati al compimento delle attività di trattamento dei dati personali;
9. I soggetti autorizzati che richiedono i dati e li ricevono, o che eseguono un qualsiasi trattamento sono comunque vincolati al rispetto del dovere di riservatezza ed sono tenuti ad eseguire tutte le misure di sicurezza per la protezione dei dati a loro trasmessi.
10. Nel caso di esercizio associato di funzioni e servizi, nonché per quelli la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del GDPR. L'accordo definisce le responsabilità di ciascuno in merito

all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
11. Il Comune impronta le attività di trattamento secondo le regole deontologiche approvate dal Garante, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare. Il rispetto delle disposizioni contenute nelle regole deontologiche costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali.

Art. 5 - Responsabile esterno del trattamento
1. Il Titolare del trattamento può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di responsabili esterni del trattamento, forniscano le garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure fisiche, tecniche e organizzative di cui all'art. 17 comma 3, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
2. I soggetti di cui al comma 1 sono tenuti a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare.
3. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, del GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
4. E' consentita la nomina di co-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; con il consenso del Titolare le operazioni di trattamento possono essere effettuate da soggetti autorizzati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del co-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 co-responsabile.
5. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
6. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee misure fisiche, tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di violazioni dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy,

nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art. 6 - Responsabile della Protezione dei Dati (RPD)

1. Il Responsabile della Protezione dei Dati (in seguito indicato con "RPD"), è designato dal Titolare. Il soggetto designato può essere un dipendente del Comune individuato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'art. 39 del RGPD, o un soggetto esterno al Comune, scelto tramite procedura ad evidenza pubblica ed in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, all'adeguata conoscenza delle strutture organizzative degli Enti locali e delle norme e procedure amministrative agli stessi applicabili, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione dell'ente. I compiti attribuiti al RPD esterno sono indicati in apposito contratto di servizio.
2. Il RPD è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare del trattamento.
3. E' possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più Enti mediante esercizio associato della funzione, nelle forme previste dal T.U.E.L., approvato con D.lgs n. 267/2000 e s.m.i.
4. Il RPD è incaricato dei seguenti compiti:
a) informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti Designati che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare 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 del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare del trattamento;
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 valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;
e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare del trattamento al Garante;
f) la revisione, in funzione della valutazione dell'impatto del registro di cui al successivo art. 10;
g) rispondere agli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR e dal presente regolamento;
h) altri compiti e funzioni a condizione che il Titolare si assicuri che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

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

- il RPD può essere invitato a partecipare alle riunioni di coordinamento dei Responsabili di Settore che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD 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 RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

6. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

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

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

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

8. Il Titolare del trattamento fornisce al RPD le risorse necessarie per assolvere i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente, e per accedere ai dati personali ed ai trattamenti. In particolare, è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Responsabili di Settore designati al trattamento e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), del bilancio di previsione e del PEG;
- tempo sufficiente per l'espletamento dei compiti affidati al RPD;
- supporto adeguato in termini di infrastrutture (sede, attrezzature, strumentazione) e, ove necessario, di personale;
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

9. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

10. Il RPD non può essere rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti.

11. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare del trattamento.

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

Art. 7 – Amministrazione del Sistema informatico

1. Per il conseguimento degli obiettivi di sicurezza informatica previsti dal C.A.D. di cui al successivo art. 17 comma 1, il Titolare, oltre al Responsabile per la transizione al digitale di cui all'art. 17, comma 1 *sexies* del C.A.D., si avvale di un dipendente dotato delle specifiche competenze informatiche, quale Designato per l'amministrazione del sistema informatico, con la precipua funzione di collaborare alla gestione e manutenzione dei sistemi informatici, con particolare riferimento alle misure tecniche predisposte dal Titolare atte a garantire un livello di sicurezza adeguato al rischio connesso ai trattamenti dei dati personali effettuati dall'Ente.

2. Il Designato, in particolare:

a) gestisce gli accessi condizionati al sistema informatico, attribuendo le credenziali ai soggetti autorizzati;

b) collabora con il Titolare per la predisposizione delle Istruzioni operative atte a garantire la sicurezza informatica;

c) propone al Titolare l'adeguamento periodico delle misure tecniche in relazione all'evoluzione tecnologica dei sistemi di ICT ed al rischio connesso al trattamento dei dati personali;

d) collabora con il Titolare e con i Designati al trattamento per verificare la corretta implementazione delle misure tecniche atte a garantire la sicurezza dei trattamenti dei dati personali;

e) assiste – se richiesto - il Titolare nell'esecuzione della D.P.I.A..

3. Qualora l' Ente non sia dotato di personale con le specifiche competenze informatiche, o a cui non possa assegnare le attività elencate, potrà ricorrere o al personale di altro Ente pubblico, a mezzo apposita convenzione, o a personale esterno individuato a mezzo procedura ad evidenza pubblica.

Art. 8 – Designato al trattamento

1. Ciascun Responsabile di Settore in cui si articola l'organizzazione dell'Ente, è nominato "Designato al trattamento" dei dati personali ricevuti dall'interessato o da terzi nell'ambito dei procedimenti amministrativi facenti capo all'articolazione organizzativa di rispettiva competenza. Alla nomina di cui sopra provvede il Titolare del trattamento mediante proprio provvedimento.

2. Il Designato è tenuto a mettere in atto le adeguate misure fisiche, tecniche e organizzative di cui al successivo art. 17, comma 3°, volte a garantire che i trattamenti siano effettuati in conformità al GDPR.

3. Le funzioni dei Designati in materia di trattamento e tutela dei dati personali, ai sensi del GDPR, sono le seguenti:

a) censire e monitorare costantemente le singole attività di trattamento dei dati personali facenti capo al Settore;

b) individuare eventuali attività di trattamento non previste all'interno del registro delle attività di trattamento predisposto dall'ente ai sensi dell'art. 30 del GDPR al fine di consentite il costante aggiornamento dello stesso;

c) segnalare le fattispecie di trattamento di cui al punto precedente al responsabile della protezione dei dati (RPD) designato dall'ente ai sensi dell'art. 37 e seguenti del GDPR;

d) assicurare la legittimità delle attività di trattamento dei dati personali ponendo in essere le adeguate misure fisiche, tecniche e organizzative di sicurezza individuate dal Titolare, dimostrabili e coerenti con quanto riportato nel registro delle attività di trattamento;

e) individuare con apposito atto di nomina le singole figure soggettive dei collaboratori interni al rispettivo Settore, incaricate delle attività di trattamento dei dati personali di competenza, per le stesse finalità di cui all'art. 4 par. 1, lett. 10, del GDPR;

f) vigilare sulla azioni dei soggetti incaricati di cui al precedente punto e garantirne la legittimità del trattamento dati personali;

g) segnalare tempestivamente al Titolare le opportune azioni correttive in caso di riscontrate violazioni delle misure tecnico- organizzative di cui al precedente punto d);

h) individuare gli eventuali soggetti responsabili del trattamento per conto del titolare ex art. 28 del GDPR, con conseguente definizione puntuale degli obblighi dello stesso all'interno di apposito contratto/atto giuridico secondo quanto previsto dal citato art. 28;
i) sollecitare l'intervento del responsabile della protezione dei dati (RPD) designato dal Comune in tutti i casi in cui si verifichi la necessità di specifiche azioni nel suo ruolo di supervisore/consulente/garante del sistema di gestione di tutela dati del Comune, ai sensi dell'art. 37 e seguenti del GDPR;
l) garantire il rispetto dei diritti del soggetto interessato e fornire adeguate informative allo stesso ai sensi degli articoli 12, 13 e 14 del GDPR, acquisendone il consenso nei casi in cui il trattamento non rientri nelle previsioni dell'art. 6 del GDPR, o i dati acquisiti rientrino nelle particolari categorie di cui all'art. 9 comma 1° del GDPR, e non sussistano ragioni giuridiche che comportino la non necessità del consenso dell'interessato;
m) proporre al Titolare eventuali nuove misure di sicurezza organizzative del trattamento non rientranti nelle specifiche competenze dell'Amministratore del Sistema informatico;
n) proporre al Titolare l'aggiornamento del Registro dei trattamenti con le eventuali nuove categorie di interessati e di dati personali afferenti alle attività del proprio Settore.

Art. 9 – Incaricati del trattamento
1. I soggetti nominati quali Designati al trattamento di cui al superiore punto provvedono a nominare gli Incaricati del trattamento da individuare, con apposito atto, tra le singole figure soggettive dei collaboratori, dipendenti od in applicazione, nel rispettivo Settore, cui affidare delle attività di trattamento dei dati personali nei procedimenti di rispettiva competenza, per le stesse finalità di cui all'art. 2 *quaterdecies*, comma 1°, Codice privacy;
2. I soggetti Incaricati devono assicurare la legittimità delle attività di trattamento dei dati personali ponendo in essere le adeguate misure fisiche, tecniche e organizzative di sicurezza, nonché le istruzioni operative emanate dal Titolare.

TITOLO III – Attività del Titolare

Art.10 - Registro delle attività di trattamento
1. Il Titolare tiene un registro delle attività di trattamento ai sensi dell'art. 30 del GDPR.
2. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
a) i dati di contatto del Titolare del trattamento e del soggetto Designato ai sensi del precedente art. 8, comma 1, dell'eventualmente contitolare del trattamento, nonché del RPD;
b) le finalità del trattamento;
c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza fisiche, tecniche ed organizzative del trattamento adottate come da successivo art. 17.
3. Il Registro è tenuto dal Titolare presso gli uffici della struttura organizzativa del Comune in formato digitale/cartaceo; nello stesso registro possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.
4. Il Titolare del trattamento, sotto la propria responsabilità, può delegare ad un soggetto Designato al trattamento di cui al precedente art. 8 il compito di tenere il Registro.
5. Il Titolare del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto alla tenuta del registro ogni elemento necessario alla regolare tenuta ed aggiornamento del registro stesso.

Art. 11 – Sistemi di I.C.T. – Pubblicazione degli atti e Amministrazione trasparente

1. Il Comune, nell'ambito delle proprie finalità istituzionali e di divulgazione delle informazioni al pubblico, implementa un proprio Web Site Internet accessibile a chiunque ed una rete intranet con accesso condizionato ai soggetti autorizzati.
2. Il Comune può consentire l'accesso a soggetti pubblici/privati portatori di interessi di natura pubblica, previa stipula di apposita convenzione, con accreditamento alla propria rete intranet per l'accesso a documenti informatici e dati personali anche in forma massiva. I soggetti autorizzati a tale accesso assumono la qualifica di Responsabili del trattamento e sono obbligati al rispetto delle norme del GDPR, del Codice privacy e del presente regolamento.
3. Il Titolare predispone un'apposita informativa ai sensi dell'art. 13 del GDPR per descrivere le modalità e le finalità del trattamento dei dati personali degli interessati raccolti tramite il portale dell'ente (Policy privacy), con riferimento all'eventuale utilizzo di sistemi di profilazione automatizzati (cookie) o di login per l'accesso ai servizi on-line previa registrazione.
4. Per le finalità indicate dalla Legge 69/2009, tutti i documenti pubblicati all'Albo pretorio on - line, salvo quelli trasmessi da altri enti, devono essere firmati con firma elettronica qualificata o firma digitale, da parte del Responsabile del procedimento che ha generato l'atto o da parte del Responsabile della transizione al digitale. La pubblicazione deve protrarsi per il solo tempo previsto dalla legge per lo specifico documento, ed al compimento il documento dovrà essere rimosso.
5. In tutti i casi di pubblicazione obbligatoria di atti disposta da norme di legge o di regolamento, ovvero per gli effetti costitutivi o di pubblicità degli stessi, qualora vi sia un trattamento di dati personali devono rispettarsi i principi di necessità, correttezza, esattezza, completezza, indispensabilità, pertinenza e non eccedenza, avuto riguardo ai destinatari dell'atto in pubblicazione (*erga omnes o ad personam*), adottando la misura di sicurezza della pseudonimizzazione o cifratura (art. 32, comma 1°, lettera a) del GDPR), ed omettendo ogni riferimento ai dati particolari (art. 9, par. 1, del GDPR). Detta misura non si applica nel caso in cui i dati personali siano stati comunicati dall'interessato con un atto processuale o stragiudiziale, ed il Titolare abbia adottato l'atto in pubblicazione per tutelare i propri diritti od interessi legittimi.
6. In casi particolari (es. atti adottati in procedimenti nei confronti di minori, disabili, anziani, infermi di mente e richiedenti asilo), quando con la pubblicazione dell'atto siano messi a rischio i diritti e le libertà fondamentali dell'interessato, la pubblicazione deve essere omessa o comunque eseguita con oscuramento dei dati personali dell'interessato o di quelli che siano idonei - anche indirettamente - a rivelarne l'identità o altri dati personali, con sintetica motivazione da apporre, da parte del Responsabile del procedimento o della Transizione al digitale, in calce al documento originale.
7. Per le finalità di pubblicità e trasparenza disposte dal D.Lgs. n. 33/2013 sono pubblicati in apposite sezioni del portale internet dell'ente gli atti, i documenti, le informazioni riguardanti la gestione dell'ente, tra cui: gli incarichi agli amministratori in società o enti, i contratti di appalto di lavori, servizi e forniture, le sovvenzioni, i compensi ai dirigenti, ecc.. Qualora la pubblicazione comporti un trattamento di dati personali di persone fisiche, dovranno essere opportunamente contemperati l'obbligo di pubblicità e trasparenza con il diritto alla riservatezza ed alla protezione dei dati personali dell'interessato.
8. Nel caso di richiesta di accesso civico riguardanti dati, informazioni o documenti oggetto di pubblicazione obbligatoria, il Comune se individua soggetti controinteressati, ai sensi dell'articolo 5-bis, comma 2, del D.Lgs 33/2013 è tenuto a dare comunicazione agli stessi, ed all'esito respingere od accogliere la richiesta eventualmente con limitazioni, pseudonimizzando i dati personali od escludendo atti e documenti.

Art. 12 – Segnalazione dei comportamenti illeciti dei dipendenti all'interno del Comune

1. I dati personali ed i documenti oggetto delle segnalazioni di condotte illecite ai sensi della legge 30 novembre 2017, n. 179 all'interno del Comune da parte dei dipendenti comunali, vengono trattati a norma dell'art. 32 del GDPR.

2. L’accesso agli atti da parte dei soggetti autorizzati è opportunamente regolamentato dalle politiche di sicurezza informatica dell’ente e dalla politiche di sicurezza più restrittive previste nel Manuale operativo per l’utilizzo del sistema di gestione delle segnalazioni.
3. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento, ovvero con reclamo ai sensi dell'articolo 77 del GDPR, qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del dipendente che segnala.
4. l’Ente si riserva di pubblicare una sintesi del numero di segnalazioni ricevute e del loro stato di avanzamento, con modalità tali da garantire comunque la riservatezza dell’identità dei segnalanti.

Art. 13 - Sistemi di controllo a distanza e di monitoraggio degli accessi ai luoghi di lavoro, mediante dispositivi elettronici.
1. Il Comune per esigenze organizzative, di sicurezza del lavoro e di tutela del patrimonio aziendale, nel rispetto dei principi di necessità, finalità, trasparenza, proporzionalità e sicurezza per il trattamento dei dati personali, e delle disposizioni dell’art. 4 Stat. Lav. e del CCNL, può istituire sistemi di video-sorveglianza senza che ne derivi un controllo a distanza dei lavoratori.
2. In tal caso l’installazione dei sistemi di controllo e monitoraggio non dovrà essere concertata con le rappresentanze sindacali.
3. Il Titolare del trattamento deve informare i lavoratori circa l'esistenza e le modalità d'uso degli strumenti di controllo, con riferimento alla finalità e alle modalità del trattamento dei dati, alla natura obbligatoria e facoltativa del conferimento dei dati, alle conseguenze di un eventuale rifiuto, ai soggetti cui tali dati possono essere comunicati.

Art. 14 – Sistemi di videosorveglianza del territorio.
1. Il Comune nell’ambito delle politiche di sicurezza sociale e di contrasto ai fenomeni di micro-criminalità tra cui atti di vandalismo o danneggiamento dei beni pubblici, nonché per l’accertamento delle violazioni delle norme del Codice della strada, può istallare sul proprio territorio sistemi di videosorveglianza, nonché sistemi di ripresa audio-video in real-time, attivabili anche da remoto, direttamente sui veicoli o sulla divisa degli Agenti della Polizia locale (bodycam).
2. Gli impianti di videosorveglianza sono finalizzati a:
a) controllare determinate aree, impianti od edifici pubblici per una tutela dei beni pubblici;
b) monitorare il traffico e gli accessi alle aree oggetto di restrizione al traffico od alla sosta (Z.T.L.).
3. Le modalità di gestione degli impianti e di trattamento dei dati ovvero: tutte le operazioni o complesso di operazioni, svolte con l’ausilio dei mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l’organizzazione, la conservazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l’interconnessione, il blocco, la comunicazione, l’eventuale diffusione, la cancellazione e la distribuzione di dati, sono disciplinate con apposito regolamento.
4. La durata della conservazione dei dati raccolti è di 7 giorni, salvo maggior periodo per comprovate esigenze previste nell’apposito regolamento, e previo parere dell’Autorità Garante. Al termine del periodo di conservazione, i dati devono essere cancellati. Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
5. La gestione del servizio di trattamento delle immagini acquisite con i sistemi di videosorveglianza può essere affidata a soggetti privati che diano garanzie per la sicurezza del trattamento dei dati personali.

Art. 15 – Open Data

1. I dati pubblici presenti nelle banche dati del Comune, prodotti o acquisiti nell'ambito dell'esercizio delle sue funzioni istituzionali, sono patrimonio della collettività che ha diritto di accedervi e di riutilizzarli liberamente, nei limiti previsti dalla legge.
2. Sulla base del principio enunciato al comma 1 del presente articolo, il Comune può rendere disponibili, sul proprio portale web dedicato ai dati aperti, i dati pubblici detenuti nelle proprie banche dati, e ne favorisce il libero riutilizzo a vantaggio della collettività per la creazione di opportunità economiche e per la promozione della partecipazione consapevole all'attività politica e amministrativa, nei limiti consentiti dalla legge.
3. Con apposito Regolamento, adottato secondo le disposizioni del Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale), e nel rispetto della normativa vigente in materia di tutela dei dati personali, nell'ambito dei dati in possesso del Comune sarà prevista:
a) l'individuazione dei dati esclusi dalla pubblicazione;
b) la pubblicazione e l'esercizio della facoltà di accesso telematico ai dati pubblici;
c) le modalità di riutilizzo dei dati pubblici.

16 – Conservazione dei dati e dei documenti informatici.

1. Il Comune nell'ambito degli obiettivi del D.lgs 445/2000 istituisce l'Archivio digitale dei documenti informatici, fatte salve le vigenti disposizioni sulla gestione e conservazione dell'archivio degli atti e documenti in formato cartaceo.
2. La gestione dell'archivio può essere demandata con apposita convenzione a soggetti pubblici o privati, i cui sistemi organizzativi e tecnici diano le opportune garanzie di sicurezza per il trattamento dei dati personali, in quanto muniti dell'apposita certificazione.
3. L'acquisizione e la conservazione dei documenti informatici è attuata secondo le linee guida AgID del 2015 e ss.mm.ii., e nel rispetto delle regole tecniche adottate con il C.A.D. (D.lgs 82/2005 - Codice per l'Amministrazione Digitale)
4. I dati personali raccolti presso l'interessato o presso terzi, con l'ausilio di strumenti informatici o su documento cartaceo, sono conservati in banche dati, informatiche e/o cartacee, anche disgiuntamente dal documento informatico a cui sono riferiti, e sono conservati per il tempo strettamente necessario alla conclusione del procedimento per il quale sono stati raccolti, o per quello eventualmente indicato nel registro delle attività di trattamento per lo specifico procedimento.
5. I dati personali aggregati al documento informatico cui sono riferiti per lo specifico procedimento sono conservati per il tempo indicato dalla legge per la conservazione del documento stesso.

TITOLO IV – Sicurezza, valutazione d'impatto, accesso agli atti e norme applicabili

Art. 17 – Misure di sicurezza

1. Il Titolare, il Responsabile e ciascun Designato al trattamento adottano le opportune misure fisiche, tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Le misure fisiche, tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure fisiche, tecniche ed organizzative che devono essere adottate dal Settore cui è preposto ciascun Designato al trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza;
- sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici;
- altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico per garantire la continuità operativa;
- istruzioni operative per i Designati al trattamento.

4. La conformità del trattamento dei dati al GDPR in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
5. Il Comune si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per suo conto ed abbia accesso a dati personali.
6. I dati di contatto del Titolare, dei Designati al trattamento e del RPD sono pubblicati sul sito internet istituzionale dell'Ente, sezione Amministrazione trasparente, oltre che nella apposita sezione "privacy".

Art. 18 - Valutazioni d'impatto sulla protezione dei dati

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 valutazione dell'impatto del medesimo trattamento (DPIA), ai sensi dell'art. 35 del GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
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.
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 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 dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori. In tal senso la DPIA deve essere sempre eseguita nel caso di trattamenti non occasionali di dati relativi a minori, disabili, anziani, infermi di mente, richiedenti asilo;
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 non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.
5. Nell'esecuzione della DPIA si devono seguire le linee guida adottate dal WP29, come recepite dall'Autorità Garante, con particolare considerazione dei seguenti criteri, salvo futuri nuovi od integrazioni:
I. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, 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"* (considerando 71 e 91);
II. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che *"hanno effetti giuridici*" o che "*incidono in modo analogo significativamente su dette persone fisiche*" (articolo 35, paragrafo 3, lettera a));
III. Monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o *"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*" (articolo 35, paragrafo 3, lettera c);
IV. Dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 GDPR (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10 GDPR;
V. Trattamento di dati su larga scala: il GDPR non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:
a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
c. la durata, ovvero la persistenza, dell'attività di trattamento;
d. la portata geografica dell'attività di trattamento;
VI. Creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
VII. Dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento;
VIII. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc.;
IX. Quando il trattamento in sé *"impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"* (articolo 22 e considerando 91).

6. 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.
7. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.
8. Il soggetto Autorizzato al trattamento deve assistere il Titolare nella conduzione della DPIA fornendogli ogni informazione necessaria.
9. L'Amministratore dei sistemi informativi fornisce supporto al Titolare per lo svolgimento della DPIA.
10. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
11. 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 25 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.
12. Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica.
13. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

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

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

14. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
15. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.
16. 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. 19 - Violazione dei dati personali
1. Il Titolare in presenza di una violazione di dati personali (*Data breach)* ove ritenga probabile che dalla stessa possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy.
La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
2. 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:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari, ecc.).

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

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

4. La notifica deve avere il contenuto minimo previsto 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.
5. 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. 20 – Diritti dell'interessato

1. L'interessato ha diritto:

a) ai sensi degli articoli 13 e 14 del GDPR di ricevere dal Titolare le informazioni, relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro;

b) ai sensi degli articoli da 15 a 22 del GDPR, di accedere, di chiedere la rettifica o la cancellazione in tutto o in parte, ai propri dati personali, nonché la loro portabilità in formato accessibile ed in autonomi supporti analogici o informatici qualora gli stessi non siano più necessari per la formazione, validità e/o efficacia del documento amministrativo informatico/analogico per il quale sono stati forniti; di essere informato sull'eventuale processo decisionale automatizzato, e di potervisi opporre;

c) ai sensi dell'art. 34 del GDPR di ricevere da Titolare la comunicazione della violazione dei dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

2. L'interessato può esercitare i propri diritti inviando una richiesta alla casella di P.E.C. del Comune. Nell'oggetto l'interessato dovrà specificare il diritto che si intende esercitare, per quale finalità sa o suppone che i suoi dati siano stati raccolti dal Comune e dovrà allegare, se la richiesta non proviene da una casella pec intestata all'interessato, la richiesta sottoscritta ed un proprio documento di identità.

3. L'interessato può contattare il RPD per segnalare le problematiche connesse all'esercizio dei propri diritti mediante una casella di posta elettronica dedicata. Il RPD ricevuta la segnalazione dall'interessato circa la violazione dei propri diritti provvede sollecitamente a contattare il Titolare e/o il soggetto Designato al trattamento per assumere tutte le necessarie informazioni atte a verificare la fondatezza della segnalazione. In caso affermativo suggerisce al Titolare e/o al Designato al trattamento la soluzione alla problematica segnalata, dandone comunicazione all'interessato entro il termine di 30 giorni dal ricevimento della segnalazione.

4. L'interessato ha diritto, ai sensi all'articolo 77 del GDPR, di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione, in caso ritenga illecito il trattamento dei propri dati personali per violazione delle norme previste dal GDPR e dal Codice Privacy.

Art. 21 Accesso ai documenti amministrativi e accesso civico

1. Fatto salvo quanto previsto dall'articolo 60 del Codice privacy, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i dati di cui agli articoli 9 e 10 del GDPR e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.

2. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal D.Lgs 33/2013.

Art. 22 – Norme applicabili e conservazione degli effetti degli atti amministrativi

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni regolamentari, si applicano le vigenti disposizioni del GDPR ed il Codice Privacy, nonché tutte le altre disposizioni speciali per gli enti pubblici.

2. Sono fatti salvi gli effetti giuridici di tutti gli atti amministrativi adottati dall'Ente secondo la normativa privacy previgente, purché rispettino sostanzialmente i principi e le finalità delle vigenti norme in materia di tutela dei dati personali e del presente regolamento.

GLOSSARIO

Ai fini del presente Regolamento si intende per:

Titolare del trattamento: l'autorità pubblica (il Comune o altro ente locale) che singolarmente o insieme ad altri determina finalità e modalità del trattamento di dati personali;

Designato al trattamento: Il soggetto nominato da parte del Titolare del trattamento, ex art. 2 *quaterdecies* comma 1° Codice Privacy novellato, nella persona del Dirigente/Responsabile di Settore;

Incaricato del trattamento: il soggetto nominato dal Designato al trattamento, quale collaboratore del proprio Settore che compie attività di trattamento dati personali;

Responsabile del trattamento: il soggetto pubblico/privato che per conto del Titolare ex art. 28 del GDPR esegue il trattamento dei dati, la cui nomina spetta al Titolare su individuazione del singolo Responsabile di Settore con conseguente definizione puntuale degli obblighi dello stesso all'interno di apposito contratto/atto giuridico secondo quanto previsto dallo stesso art. 28 del GDPR.

Responsabile della Protezione Dati (RPD o DPO – Data Protection Officer nella accezione inglese): la figura professionale con funzioni di assistenza del titolare nominato ai sensi dell'art. 37 GDPR (cfr. considerando 97 del regolamento).

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

DPIA - Data Protection Impact Assessment – Valutazione d'impatto sulla protezione dei dati: procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali;

Garante Privacy: l'Autorità Garante per la protezione dei dati personali istituito dalla Legge 31.12.1996 n. 675, quale autorità amministrativa pubblica di controllo indipendente. L'organizzazione dell'ufficio del Garante per la privacy e le competenze sono individuate nel Codice Privacy (D.lgs 196/2003).

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

Categorie di interessati: cittadini residenti e non; minori di anni 16; elettori; contribuenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; soggetti portatori di interessi nei procedimenti amministrativi; destinatari di atti e provvedimenti; utenti di servizi generali o di prestazioni a domanda individuale; soggetti parti contraenti in rapporti di diritto privato; altro;

Categorie di destinatari: persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.

Categorie di dati personali: dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale; dati inerenti lo stile di vita; situazione economica, finanziaria, patrimoniale, fiscale; dati di connessione: indirizzo IP, login, altro; dati di localizzazione: ubicazione, GPS, GSM, altro;

Finalità del trattamento: esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico; la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica; l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune; adempimento di un obbligo legale al quale è soggetto il Comune; esecuzione di un contratto con i soggetti interessati; altre specifiche e diverse finalità;
Misure fisiche, tecniche ed organizzative: pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi; sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso; misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico, adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso; procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
Dati particolari (sensibili): i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Trattamento dei dati personali da parte delle Autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali: i dati personali indicati all'articolo 2, comma 1, lettere a), n), o) e p), del D.Lgs 51/2018**.**
Violazione di dati personali (Data breach): si intende qualsiasi violazione di sicurezza dei dati personali che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati.