REGOLAMENTO COMUNALE SUL TRATTAMENTO DEI DATI PERSONALI, PARTICOLARI

Applicazione del Regolamento europeo n. 679 del 2016

Approvato con delibera di Consiglio Comunale n. 7 del 24.06.2020

PREAMBOLO

1. Il Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 adotta una nuova disciplina sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e abroga la direttiva 95 /46/CE.
2. Il Regolamento europeo (GDPR) obbliga le Pubbliche Amministrazioni ad adeguarsi alle nuove regole in maniera tale da assicurare un livello elevato di protezione dei dati che riguardano le persone fisiche, equivalente in tutti gli Stati membri, così da rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione.
3. Il regolamento europeo richiama l'articolo 8, paragrafo 1 della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1 del Trattato sul funzionamento dell'Unione europea, nei quali è stabilito che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
4. Per l'attuazione del regolamento U.E. è necessario il diretto coinvolgimento della P.A. poiché la normativa europea determina, *in primis* un cambiamento culturale, ponendo al centro del sistema i cittadini ai quali viene riconosciuto un livello elevato e uniforme di tutela dei propri dati personali, oltreché un maggior controllo sull'utilizzo degli stessi, con il riconoscimento di nuovi e più incisivi diritti a favore di ciascun interessato quali il diritto all'oblio, il diritto alla portabilità dei dati, il diritto ad essere informato in modo trasparente, leale e dinamico sui trattamenti effettuati, il diritto ad essere informato sulle violazioni dei propri dati personali, il diritto di essere avvertiti in caso di violazioni dei dati personali entro 72 ore, il diritto a dare mandato ad un organismo apposito per proporre reclamo in caso di violazione dei dati delle disposizioni di regolamento, nonché il diritto ad ottenere tutela risarcitoria in caso di violazione del regolamento.
5. il Regolamento, impone una forte responsabilizzazione alle Pubbliche amministrazioni poiché la protezione dei dati personali diventa un "asset strategico" delle stesse P. A. ed in quanto tale deve essere valutato prima, già nel momento di progettazione di nuove procedure, prodotti o servizi, (principi "privacy by design" e "privacy by default") e non più un mero adempimento formale.
6. Il regolamento introducendo il principio di "responsabilizzazione" (cosiddetta "accountability"), attribuisce ai titolari del trattamento, ovverosia all'autorità pubblica che determina le finalità e i mezzi del trattamento dei dati personali, il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali (articolo 5 del regolamento UE).
7. L'applicazione del principio di responsabilizzazione si lega inscindibilmente al concetto di Privacy by design, ovvero l'individuazione delle concrete misure a tutela dei dati personali che l'Ente è tenuto a porre in essere oltre alle misure minime e di carattere generale riconducibili al concetto di "privacy by default".
8. Il concetto di "accountability" esprime anche l'obbligo di rendicontazione gravante su ciascuna P.A., la quale è tenuta a dimostrare di avere adottato le misure di sicurezza adeguate ed efficaci a protezione dei dati degli interessati, nonché che tali misure sono costantemente riviste ed aggiornate e che le attività proprie dell'Ente, in particolare i trattamenti svolti sono conformi con i principi e le disposizioni del Regolamento europeo, in particolare che le misure adottate a fronte dei rischi che corrono i dati forniti dagli interessati sono efficaci ed adeguate, ciò premesso, rilevato che:

le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti e che deve essere effettuata la valutazione d'impatto dal titolare con l'assistenza del RPD, che è essenziale sia per la revisione dei processi gestionali interni all'Ente, finalizzata a raggiungere i più adeguati livelli di sicurezza nel trattamento dei dati personali prescritti dalla normativa europea e rispondenti alle effettive esigenze, nonché alla struttura organizzativa e gestionale del titolare del trattamento che in occasione dell'adozione di nuove misure tecnologiche e di gestione dei dati, come nel caso di specie, tutto ciò premesso si adotta il qui di seguito

REGOLAMENTO

ART. 1 SCOPO E FINALITÀ

1. Il presente regolamento attua nel Comune di Pertengo i principi contenuti nel Regolamento UE 2016/679 in conformità alle norme del D. Lgs.196/2003, come modificato dal D. Lgs. del 10 agosto 2018 n. 101 (Codice Privacy), riordina la struttura organizzativa, le responsabilità, le misure tecniche, la comunicazione e la gestione delle diverse tipologie di dati personali, "particolari" e i trattamenti eseguiti dal Comune.
2. Il trattamento dei dati nel Comune di Pertengo ha base giuridica nelle legge sia nello svolgimento delle funzioni istituzionali, che nell'esercizio del potere pubblico attribuito e per tali attività che il Comune tratta prevalentemente dati personali comuni, dati "particolari" e giudiziari, nonché ogni altra categoria di dati così come individuate agli artt. 5; 9; 10 nel Regolamento UE 2016/679 e nel D.Lgs.196/2003, come modificato dal D. Lgs. del 10 agosto 2018 n.101 artt. 2-sexies; 2-septies; 2-octies; 59; 60; 75.
4. I dati personali nel Comune sono trattati in modo lecito, corretto e trasparente e sono raccolti per le finalità determinate dalla legge e dai regolamenti che sono esplicite e legittime, e i trattamenti avvengono in modo non incompatibile con le finalità istituzionali attribuite.
5. I dati sono trattati nel Comune in modo adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono trattati e di norma secondo il criterio di «minimizzazione dei dati». Dei dati è costantemente verificata l'esattezza e, quando è necessario l'aggiornamento. Nel trattamento il Comune adotta tutte le misure tecniche adeguate e ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
6. La limitazione della conservazione dei dati in Comune è volta a consentire l'identificazione degli interessati solo per l'arco di tempo necessario nel quale è in atto il trattamento che, di norma, non può essere mai superiore alle finalità per le quali i dati stessi sono trattati.
7. Nel rispetto delle singole leggi di settore che prevedono la conservazione per periodi diversi per quelli stabiliti è possibile la conservazione dei dati per periodi più lunghi in relazione alla tipicità dei singoli procedimenti amministrativi, di legittimo interesse del Comune a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica quando necessario, e a garanzia per gli utenti in ragione delle attività che istituzionalmente sono poste in capo al Comune.

Art. 2 Disposizioni generali

1. Il Comune nel trattare i dati osserva la vigente normativa Europea e Nazionale, i pareri del Garante nazionale, le decisone della Commissione Europea e del GEPD. Il trattamento dei dati in Comune è sempre improntato al rispetto dei diritti e delle libertà fondamentali dell'interessato è per le finalità di interesse pubblico perseguito dall'Ente.

2. Il Comune adegua la propria organizzazione interna alla normativa sulla protezione dei dati, in senso verticale con a capo il Sindaco, titolare dei dati dell'Ente. Allo stesso rispondono i dirigenti di struttura semplice e le P.O. che sono responsabili dei trattamenti di rispettiva competenza delle strutture alle quali sono preposti. Spetta ai responsabili interni designare singoli dipendenti al trattamento. Al responsabile alla protezione dei dati spettano compiti di consulenza, controllo e collaborazione con il Titolare e con i dirigenti per ogni attività, organizzazione, innovazione e programmazione Comunale nella quale sono coinvolti dati personali.

Art. 3 Definizione di dati personali e dati particolari

1. Ai fini dell'applicazione della normative europea e nazionale a tutela delle persone fisiche e per le legittime attività di trattamento per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
2. Trattamento è qualsiasi singola operazione, svolta dal personale dipendente ed onorario del Comune che ha base giuridica in una legge o regolamento o nell'esercizio della funzione di diritto pubblico attribuita all'Ente, ovvero l'insieme delle operazioni, compiute sia attraverso la forma analogica che digitale e quindi con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come e che consistono nella raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione di dati personali trattati in Comune.
3. Il Comune si conforma al divieto del trattamento dei dati "particolari" di cui all'art. 9 del GDPR e, in assenza di previsione derogatoria ovvero dell'espresso consenso dell'interessato, il personale del Comune si astiene dal trattare dati "particolari" che direttamente o indirettamente siano idonei a far rilevare:

- l'origine razziale o etnica dei soggetti i cui dati vengono trattati;
- le loro opinioni politiche;
- le loro convinzioni religiose o filosofiche;
- l'appartenenza sindacale anche per i dipendenti interni;
- i loro dati genetici;
- i loro dati biometrici che identificano la persona fisica,
- dati relativi alla salute;
- alla vita sessuale o all'orientamento sessuale.

4. Il Comune è legittimata a trattare i dati "particolari", di cui al precedente comma 3, quando ricorre una delle seguenti condizioni:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali per una o più finalità specifiche in relazione ai compiti pubblici attribuiti al Comune;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici attribuiti all'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, sulla base del diritto dell'Unione o Nazionale, fatte salve le garanzie per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato quando questi sono reperibili sul web tramite i motori di ricerca o trasmessi al Comune con il Curriculum per la partecipazione a selezioni pubbliche;

e) il trattamento è necessario per gli interessati o terzi controinteressati per fare accertare, esercitare o difendere un diritto in sede giudiziaria;

f) il trattamento è necessario per motivi di interesse pubblico rilevante in relazione alle attribuzioni al Comune derivanti da leggi regolamenti o disposizioni dirigenziali motivate dal legittimo interesse dell'Ente;

g) il trattamento è necessario in quanto è relativo alla raccolta, esame e trasmissione di dati raccolti per le finalità nell'ambito dei compiti istituzionali attribuiti al Comune della capacità lavorativa del dipendente, diagnosi, assistenza;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, storica o a fini statistici.

5. Il Comune tratta i dati in deroga al divieto di cui al co. 4 lett. f) per una o più delle fattispecie consentite dall'art. 2-sexies del D. Lgs. 196/2003 in relazione ad una o più finalità consentite per il trattamento dei dati personali particolari, sulla base di provvedimenti motivati ovvero nell'esercizio di un potere pubblico o istituzionale o nell'ambito di provvedimenti istruttori che hanno base giuridica nella legge e nei regolamenti.

Art. 4 Titolare del trattamento

1. Per i trattamenti di legge e la tutela delle persone fisiche per le finalità istituzionali il Sindaco è il titolare dei dati personali contenuti nelle banche dati automatizzate o cartacee.

2. Il Sindaco determina le finalità e i mezzi del trattamento, predispone le line di Policy Privacy del Comune, adotta il regolamento interno privacy su proposta del DPO.

3. Al Sindaco spetta inoltre il compito di:

a. Adottare, sentito i responsabili al trattamento della struttura interessata ed il DPO, le misure tecniche ed organizzative adeguate volte a garantire un livello di sicurezza al rischio del trattamento dei dati in Comune.

b. Tenere e implementare, anche per mezzo di uno o più dipendenti interni il registro dei trattamenti.

c. Vigilare, anche attraverso il Responsabile incaricato, sul registro delle attività di trattamento in capo ad ogni struttura dell'Ente.

d. Attestare, se richiesto dal Garante o dall'A.G., che i trattamenti sono conformi ai principi e alle disposizioni di legge del Regolamento UE e delle prescrizioni del Garante.

e. Monitorare periodicamente, mediante gli amministratori di Sistema, l'efficacia delle misure di sicurezza tecniche e fisiche adottate in Comune sentito il parere del DPO.

f. Mettere il registro dei trattamenti a disposizione dell'autorità Garante facendosi supportare all'uopo anche uno o più dei responsabili designati.

g. Nominare i responsabili del trattamento, attribuendo agli stessi la facoltà di nominare sub-responsabili e di designare dipendenti della singola struttura al trattamento sulla base degli atti predisposti dal DPO.

h. Stipulare contratti di nomina di responsabili esterni per i servizi dell'Ente esternalizzati, aggiudicati, affidati, sentito il parere del DPO.

i. Sottoscrive i contratti di contitolarità sentito il DPO.

j. Stipula protocolli d'intesa con Enti, Procure, Tribunali, Corti, Polizia di Stato e arma dei Carabinieri, Guardia di Finanza per ogni attività che comporta scambio di dati personali e accesso a banche dati dell'Ente in relazione ai compiti ispettivi e di controllo ambientale attribuito per legge.

k. Organizzare ogni altra attività e attribuire compiti e funzioni in materia di protezione dei dati personali.

l. Nomina, ai sensi dell'art. 7, comma 6, D.lgs. 165/2001, nel rispetto delle previsioni del GDPR e tenuto conto delle specifiche competenze e della pregressa esperienza, il Responsabile della protezione dati individua le risorse umane e finanziarie necessarie nonché la struttura per le attività del RPD.

m. Adotta il Piano della sicurezza del patrimonio informativo, le politiche di sicurezza, le metodologie di analisi del rischio privacy e di valutazione di impatto, le linee guida per l'utilizzo dei dispositivi fissi e mobili.

n. Presiede il Gruppo di lavoro per la gestione delle violazioni di dati personali (Data Breach) composto dai responsabili incaricati, l'Amministratore di Sistema, il RPD.

o. Ogni altra questione ad esso demandata dallo Statuto, dalla legge o dai regolamenti in materia di protezione dei dati personali dei dirigenti delle strutture amministrative.

p. predispone sentito il RPD i modelli facsimile di lettera di autorizzazione al trattamento dei dati personali e di affidamento della custodia di particolari archivi, chiavi o credenziali di autenticazione e impartisce le relative istruzioni ai soggetti autorizzati al trattamento di dati personali.

q. Autorizzare i dirigenti delle strutture amministrative dell'Ente ai trattamenti di dati personali nell'ambito delle funzioni istituzionali svolte e di attribuire agli stessi, compresa l'individuazione dei dipendenti, dei tirocinanti e degli altri soggetti da autorizzare al trattamento dei dati personali, necessari per lo svolgimento delle rispettive mansioni, mediante trasmissione di apposita lettera di autorizzazione e delle istruzioni.

Art. 5 Registro delle attività di trattamento

1. Il Sindaco tiene, sotto la propria responsabilità, il Registro delle attività di Trattamento la cui compilazione e implementazione può assegnare a un dirigente interno, o ad uno o più dipendenti.
2. Sono sub-responsabili per ogni struttura i dirigenti che sono tenuti all'implementazione del registro dei trattamenti della struttura, con la facoltà di designate dipendenti alla tenuta del registro stesso della struttura.

3. Il Registro del titolare, è redatto in forma scritta, anche in formato elettronico, ed è unico per tutto l'Ente, ed è messo a disposizione, a richiesta, dell'Autorità Garante per la Privacy, per ispezioni e controlli ai fini della correttezza nella gestione e trattamento dei dati personali.
4. Il Registro ha una funzione descrittiva e dovrà essere implementato da ogni struttura dirigenziale. Sarà tenuto nelle forme e con le modalità sentito il Responsabile alla Protezione dei dati, e contiene, le informazioni previste dall'art. 30 del Regolamento UE e le altere specifiche relative ai trattamenti in capo al Comune.

Art. 6 Responsabile del trattamento

1. I Responsabili del trattamento sono individuati tra i dirigenti e le Posizione Organizzative (P.O.) o i dipendenti dell'Ente e sono nominati con atto giuridico vincolante dal titolare. La mancata accettazione della nomina costituisce illecito contrattuale con le conseguenze di legge ove non sia possibile attribuire mansioni che non comportano trattamento di dati personali.
2. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il responsabile del trattamento della struttura, sentito il RPD, consiglia al titolare di mette in atto misure tecniche e organizzative adeguate.
3. Il responsabile adempie agli obblighi di trasparenza e vigilanza, prescritti dal titolare nell'atto giuridico di nomina mettendo a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi imposti dall'art. 28 del Regolamento, ed è obbligato a tenere il registro dei trattamenti svolti della struttura al quale è preposto (ex art. 30, paragrafo 2, GDPR).
4.Il responsabile ai trattamenti ha l'obbligo di garantire la sicurezza dei dati, di adottare misure adeguate al rischio (art. 32 GDPR) incluse le misure di *privacy by design e by default* e garantire la riservatezza dei dati ed è tenuto ad informare il titolare delle violazioni avvenute e provvedere alla cancellazione dei dati alla fine del trattamento.
5. Il responsabile del trattamento ha l'obbligo di coadiuvare il titolare nell'adozione delle misure tecniche e organizzative imposte dai processi di innovazione tecnologica, 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.
6.Il responsabile al trattamento indica al titolare, sentito il RPD, alcune misure di sicurezza utili per ridurre i rischi del trattamento, quali la pseudonimizzazione e 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. Il responsabile può dimostrare di avere adottato garanzie sufficienti anche attraverso l'adesione a codici deontologici ovvero a schemi di certificazione privacy.

7. Il responsabile ha l'obbligo, d'intesa con il RPD, di avvisare, assistere e consigliare il titolare ed è tenuto a consentire e contribuire alle attività di revisione, comprese le ispezioni e *audit*, realizzate dal titolare del trattamento, dovrà avvisare il titolare se ritiene che un'istruzione ricevuta viola qualche norma in materia di *privacy e Cyber Security*, dovrà prestare assistenza al titolare per l'evasione delle richieste degli interessati, dovrà avvisare il titolare in caso di violazioni dei dati, e assisterlo nella conduzione di una valutazione di impatto (DPIA).

Art. 7 Incaricati del trattamento

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
2.Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.
3. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Titolare o del Responsabile del trattamento dati e i designati devono attenersi scrupolosamente alle istruzioni impartite.
4. La designazione è effettuata, dal titolare o dal Responsabile, sentito il RPD, per iscritto e l'atto di designazione deve individuare puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Art. 8 Responsabile del trattamento dati informatici e telematici (D.I.T.)

1. La responsabilità del trattamento dei dati informatici e telematici è attribuita al Responsabile dei Sistemi Informativi e Servizi Informatici. Le competenze del Responsabile riguardano l'attività di controllo e gestione degli impianti di elaborazione o di sue componenti, di basi di dati, di reti, di apparati di sicurezza e di sistemi di software complessi (nella misura in cui consentono di intervenire su dati), l'individuazione e attuazione di tutte le procedure fisiche, logiche e organizzative per tutelare la sicurezza e la riservatezza nel trattamento dei dati informatici.
2. Il Responsabile del trattamento dati informatici e telematici designa per iscritto con provvedimento motivato, un numero limitato, di amministratori di sistema e di amministratori di macchina, previa individuazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3.Il Responsabile del trattamento dati informatici e telematici predispone - per le parti relative alla sicurezza informatica, ai trattamenti di dati personali con mezzi elettronici e digitali e allo sviluppo delle applicazioni informatiche - proposte per il:

a. Piano della sicurezza del patrimonio informativo e della protezione dei dati personali;
b. Il Piano per la gestione delle violazioni di dati personali di competenza;

c. Il Piano di attuazione delle politiche di sicurezza relative ai trattamenti informatici/digitali di dati personali, in conformità delle line guida del RDP e dell'Agenzia per l'Italia Digitale;

d. Un Piano di supporto all'attività delle strutture del Comune nell'applicazione delle politiche di sicurezza informatica, anche attraverso l'identificazione di specifiche soluzioni tecniche e procedurali e l'individuazione delle misure di protezione adeguate al rischio;

e. Le misure di tenuta della documentazione relativa alle misure di sicurezza applicate alle infrastrutture e alle applicazioni gestite e degli esiti degli eventuali controlli di vulnerabilità effettuati, salvo che tale compito sia stato affidato a un fornitore designato responsabile del trattamento;

f. L'elenco aggiornato e la pubblicazione dell'elenco delle banche dati informatiche come previsto dal CAD;

g. L'elenco designazione amministratori di sistema e amministratori di singole postazioni di lavoro nei limiti concordati con il titolare e il RPD in conformità ai provvedimenti generali del Garante dei dati personali;

h. Le attività previste nel Piano di gestione delle violazioni di dati personali (Data Breach) e delle attività necessarie per l'applicazione della metodologia di analisi dei rischi o per l'eventuale valutazioni di impatto sulla protezione dei dati, sia sui trattamenti già in corso, sia all'avvio di nuovi trattamenti con strumenti informatici o dell'utilizzo di nuovo tecnologie, in conformità ai principi della protezione dei dati fin dalla progettazione (privacy by design) e della protezione per impostazione predefinita (privacy by default).

4.Il dirigente, ovvero la P.O. o il dipendente dell'Ufficio ICT svolge i compiti e le funzioni raccordandosi con il RPD con il titolare, o suo delegato, con il Responsabile per la Transizione al digitale è con gli altri component del Gruppo di lavoro privacy.

Art. 9 Gruppo di lavoro e referente privacy

1.Il Referente Privacy è un dipendente del Comune che coadiuva il Titolare nell'espletamento dei molteplici compiti afferenti la tematica dei dati personali svolti dall'Ufficio e per il Sindaco si interfaccia con il Responsabile per la Protezione Dati e al quale assicura i mezzi finanziari ed organizzati necessari per lo svolgimento delle attività, ne condivide l'Agenda delle riunioni alle quali il RPD deve necessariamente essere presente quando vengono adottati procedimenti innovativi o innovazione tecnologiche ed organizzative dell'Ente.

2. L'ufficio Privacy è struttura di coordinamento gli adempimenti in materia di trattamento dei dati personali propone gli schemi di provvedimento in materia di protezione dei dati personali preparati dai dirigenti competenti e supervisionati e con l'avallo definitivo del RPD.

3. Convoca la riunione del tavolo di lavoro in occasione violazioni di dati personali, della valutazione d'impatto sulla protezione dei dati, della consultazione preventiva, nonché delle altre comunicazioni al Garante della protezione dei dati personali, fatto salvo quanto di competenza diretta del RPD.

4. Ai sensi dell'art. 2-quaterdecies del d.lgs. 196/2003, il referente privacy è il soggetto competente ad adottare, sentito il RPD:

a. l’elenco dei trattamenti di dati personali rientranti nella titolarità del Comune assegnati a ciascun titolare di incarichi dirigenziali, secondo le competenze assegnate nei provvedimenti organizzativi dall’Ente e in coerenza con il Registro delle attività di trattamento;

b. le istruzioni per il trattamento dei dati personali, in conformità al Piano della sicurezza del patrimonio informativo e della protezione dei dati personali, e i modelli per l’autorizzazione del personale al trattamento dei dati necessari per lo svolgimento delle attività di ufficio;

c. le procedure per garantire l’esercizio dei diritti degli interessati sulla base della previsione dei successivi artt. 18, 19, 20;

d. le procedure relative agli amministratori di sistema e i processi di gestione e progettazione di nuovi servizi o nuovi trattamenti, basati sui principi della protezione dei dati fin dalla progettazione (privacy by design) e della protezione per impostazione predefinita (privacy by default);

e. le procedure di designazione dei responsabili del trattamento e gli schemi degli atti negoziali da proporre al titolare, sentito il RPD e sulla base dei modelli ed atti dallo stesso proposti;

f. propone al titolare, sentito obbligatoriamente il RPD I cui pareri sono vincolanti, le modifiche organizzative, tecnologiche e di sicurezza che derivano da provvedimenti e delle prescrizioni del Garante per la protezione dei dati personali,

g. ogni altra informazione che non rientra nella competenza esclusiva del RPD in merito allo stato di adeguamento della privacy nell’Ente e monitoraggio dell’attività di formazione e del Gruppo di lavoro interno.

Art. 10 Responsabile della Protezione dei dati

1.Il RPD ha in Comune un ruolo fondamentale per la promozione della cultura della protezione dei dati e per l’attuazione del GDPR e dei principi fondamentali del trattamento; i diritti degli interessati; la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita; i registri delle attività di trattamento; la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali; le misure tecniche; la modulistica la consulenza legale in materia di privacy e protezione dei dati.

2. In ottemperanza all’art. 39 comma 1 del Reg. UE 2016/679 il DPO è incaricato di:

a. informare e fornire consulenza al titolare del trattamento e ai responsabili del trattamento, ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dall’applicazione della normativa;

b. sorvegliare sull’attuazione in Comune delle disposizioni del Regolamento UE sulla protezione dei dati, le disposizioni degli Stati membri relativamente alla protezione dei dati, delle politiche del titolare in materia di protezione dei dati personali, la formazione del personale, le attività di controllo;

c. cooperare con l’autorità di controllo, ne è il referente e fungere da punto di contatto per questioni del trattamento, tra cui la consultazione preventiva di cui all’art. 36 del Reg. UE 2016/679;

d. vigilare sul Comune per le attività alla stessa spettante in materia di Registro dei trattamenti. Supporta la revisione delle informative e del consenso per conformarle al GDPR;

e. svolgere attività di consulenza preventiva in materia di protezione dei dati, monitorare e consigliare le politiche di protezione dei dati adeguate alle specifiche attività svolte dal Comune, esprimere parere sui contratti tra contitolari e tra titolare e responsabili;

f. fornire supporto al Titolare in ordine alla valutazione d'impatto sulla protezione dei dati e vigila sullo svolgimento ai sensi dell'articolo 35 del Regolamento;

g. svolgere le funzioni comunque assegnate dalla normativa vigente e nell'esecuzione dei compiti il RPD compie una valutazione dei rischi tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo e nella valutazione del "rischio" è titolato a conduce una valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment - DPIA);

h. gestire i tentativi e le violazioni dei dati personali (Data Breach) e partecipare alle riunioni del Gruppo di lavoro;

i. monitorare e gestire i reclami sulla base della procedura fissata nel presente regolamento, partecipare alla redazione dei codici di condotta ed esprime parere sulle certificazioni.

3. Il conferimento dell'incarico al RPD è fatto con atto del Sindaco ai sensi dell'art. 5 lett. l. del presente regolamento, sulla base dell'art. 7, comma 6, D.lgs. 165/2001, previa procedura selettiva comparativa sul MEPA per i professionisti abilitati ai servizi specialistici alla P.A., in materia di privacy e protezione dei dati, tenuto conto dei seguenti requisiti: competenza dei concorrenti sulle base delle loro pregresse esperienze in materia di privacy e protezione dei dati; l'avere in corso o avere svolto incarichi, per almeno un biennio, presso almeno due Provincie o due Città capoluoghi di Provincia; o altre Istituzioni o Agenzie Pubbliche, avere specifica esperienza in materia di protezione dei dati certificate sulla base del relativo curriculum professionale.

4. Il nominativo deve essere immediatamente comunicato all'Autorità di controllo e il RPD entra nelle funzioni con la sottoscrizione del contratto.

Art. 11 Responsabile della Conservazione dei Documenti Informatici

1. Con provvedimento del Sindaco è individuato il responsabile del Comune alla conservazione dei documenti informatici, ai sensi dell'art.7 del D.P.C.M. 03.12.2013 (" Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al Decreto Legislativo n.82 del 2005") e s.m.i.

Art. 12 Trattamento dei dati nell'ambito del rapporto di lavoro pubblico

1. Per i trattamenti nell'ambito del rapporto di lavoro pubblico si rinvia all' art.111 del D. Lgs. 196/2003 che prevede l'adozione di Regole deontologiche che saranno approvate dal garante ai sensi dell'articolo 2-quater del Codice Privacy, per i trattamenti dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendosi anche specifiche modalità per le informazioni da rendere all'interessato.

2. Il Comune come pubblica amministrazione può comunicare ad altre amministrazioni pubbliche i dati trattati quando la comunicazione dei dati ha base nella legge o deve essere effettuata in esecuzione di compiti di interesse pubblico ai sensi dell'art. 2 sexies del D. Lgs. 196/2003 ovvero nell'esercizio del pubblico potere attribuito e per gli obblighi previsti e volti a tutelare le esigenze della legislazione fiscale, assistenziale e previdenziale.
3. La comunicazione dei dati a terzi è consentita in forma anonima e ai fini delle politiche del lavoro e di statistica ricavati dalle informazioni relative a singoli o a gruppi di lavoratori: come il numero complessivo di ore di lavoro straordinario prestate o di ore non lavorate nelle varie articolazioni organizzative, gli importi di trattamenti stipendiali o accessori individuati per fasce o qualifiche/livelli professionali, le giornate non lavorato per motivi di salute, o per benefici di legge anche nell'ambito di singole funzioni o unità organizzative, salvo che anche tale diffusione di dati anonimi sia di pregiudizio per la libertà e dignità del lavoratore qualora individuabile.
4. Ad esclusione dei casi in cui il contratto collettivo applicabile preveda espressamente che l'informazione sindacale abbia ad oggetto anche dati nominativi del personale per verificare la corretta attuazione di taluni atti organizzativi, l'amministrazione può fornire alle organizzazioni sindacali dati numerici o aggregati e non anche quelli riferibili ad uno o più lavoratori individuabili. È il caso, ad esempio, delle informazioni inerenti ai sistemi di valutazione dell'attività dei dirigenti, alla ripartizione delle ore di straordinario e alle relative prestazioni, nonché all'erogazione dei trattamenti accessori.
5. L'amministrazione può anche rendere note alle organizzazioni sindacali informazioni personali relative alle ritenute effettuate a carico dei relativi iscritti, in conformità alle pertinenti disposizioni del contratto applicabile.

Art. 13 Modalità di comunicazione di dati personali lavoro dipendente autonomo o onorario

1. Fuori dei casi in cui forme e le modalità di divulgazione di dati personali siano regolate specificamente da puntuali previsioni di legge o regolamento, il Comune deve utilizzare forme di comunicazione individuale con il lavoratore dipendente o autonomo, il professionista, l'incaricato il nominato o designato per un attività di lavoro autonomo, onorario o stage, adottando tutte le misure più opportune per prevenire la conoscibilità ingiustificata di dati personali, in particolare se sensibili, da parte di soggetti diversi dal destinatario, ancorché incaricati di talune operazioni di trattamento[1]
2. La diffusione di dati personali riferiti ai lavoratori può avvenire quando è prevista espressamente da disposizioni di legge o di regolamento o per previsione contrattuale, anche mediante l'uso delle tecnologie telematiche[2].

[1] Esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali.
[2] Art. 3 D. Lgs 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale" .

Art. 14 Accesso agli atti amministrativi e accesso civico generalizzato

1. Fatto salvo i dati relativi alla salute, vita sessuale e orientamento sessuale, vietati, ai sensi dell'art. 9 del GDPR e fatto salvo le deroghe previste dallo stesso Regolamento UE e la deroga del legittimo interesse di cui all'art. 2-sexies del D. Lgs. 196/2003, l'accesso agli atti del procedimento amministrativo in Comune è disciplinato 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 tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Nel Comune i presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33 e ss.mm.ii.
2. Il trattamento dei dati vietati di cui al precedente comma è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale, la valutazione del livello di rango spetta al responsabile al trattamento della struttura titolare del relativo procedimento.
3. Il Comune valorizza l'utilizzo di reti telematiche per la messa a disposizione di atti e documenti contenenti dati personali (es. concorsi o a selezioni pubbliche) nel rispetto dei principi di necessità, pertinenza, minimizzazione e non eccedenza.

Art. 15 Dati relativi ai concorsi e alle selezioni pubbliche

1. Il trattamento dei dati relativi a concorsi pubblici è consentito presso il Comune in conformità del parere del Garante Privacy del 2014. Quando la selezione contiene parametri, ai fini del posizionamento in graduatoria, che direttamente o indirettamente siano idonei a recare pregiudizio alla libertà e alla dignità dei concorrenti i nominativi degli stessi dovranno essere trattati e pubblicati in forma anonima.
2. Il Comune, nel rispetto della previsione di cui al precedente co.1, può lecitamente trattare, in base a specifiche previsioni legislative o regolamentari, solo i dati personali pertinenti e non eccedenti ai fini del corretto espletamento della procedura concorsuale e della sua rispondenza ai parametri stabiliti nel bando e applicando, nella pubblicazione, i principi della minimizzazione e anonimizzazione dei dati (elenchi nominativi resi anonimi e per codice ai quali vengano abbinati i risultati di prove intermedie, elenchi degli ammessi alle prove scritte o orali, punteggi riferiti a singoli argomenti di esame; punteggi totali ottenuti).
3. Le informazioni di cui all'articolo 13 del Regolamento, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del curriculum medesimo. Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento UE 679/2016 e il consenso al trattamento dei dati personali presenti nei curricula non è dovuto e il curriculum potrà essere pubblicato salvo che, previa resa informativa, l'interessato autorizzi espressamente la pubblicazione.

Art. 16 Trattamenti basati sul consenso dell'interessato

1. Qualora il trattamento sia basato sul consenso, il Comune deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali in relazione alla finalità specifica per le quali lo ha reso. Il consenso può essere dato oralmente o per iscritto, anche attraverso mezzi elettronici ma deve essere espresso in forma comprensibile chiaro ed inequivocabile.
2. Quando l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali può essere effettuato solo per la finalità specifica per la quale è stato reso.
3. Il consenso reso per uno dei trattamenti di cui all'art. 9 del GDPR 679/2016 è sempre revocabile salvo che il diritto dell'Unione o degli Stati membri disponga espressamente che l'interessato non possa revocare il consenso reso.
4. L'interessato ha, per i dati diversi di cui all'art. 9 del GDPR, il diritto di revocare il proprio consenso in qualsiasi momento, la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca, ma legittimamente comporta che laddove il servizio non posso essere più reso, perché il trattamento è essenziale per il servizio reso lo stesso non sarà più reso, previa idonea informativa all'interessato revocante.
3.Per le pubbliche amministrazioni la base normativa sostituisce il presupposto del consenso, pertanto i soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali.

Art. 17 Diritti degli interessati riconosciuti dall'Ente

1.Gli interessati esercitano i loro diritti facendo ricorso alla modulistica pubblicata sul sito dell'Ente e nel rispetto delle norme previste nel Codice per l'esercizio dei diritti dell'interessato pure pubblicato sul sito istituzionale dell'Ente.
2.Il Diritto di accesso dell'interessato ex art. 15 del Regolamento UE 2016/679 si sostanzia nel diritto dell'interessato di ottenere dal titolare conferma che sia o meno in corso un trattamento dei propri dati personali e, in tal caso, l'accesso alle informazioni espressamente previste dall'articolo citato, tra cui a titolo esemplificativo e non esaustivo le finalità del trattamento, le categorie di dati e destinatari, il periodo di conservazione, l'esistenza del diritto di cancellazione, rettifica o limitazione, il diritto di proporre reclamo, tutte le informazioni disponibili sull'origine dei dati, l'eventuale esistenza di un processo decisionale automatizzato ai sensi dell'art. 22 del Regolamento, nonché copia dei propri dati personali.
3. Il Diritto di rettifica ex art. 16 del Regolamento UE si sostanzia nel diritto dell'interessato di ottenere dal titolare la rettifica e/o l'integrazione dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo.
4. Il Diritto alla cancellazione "diritto all'oblio" ex art. 17 del Regolamento UE si sostanzia nel diritto dell'interessato alla cancellazione dei propri dati personali senza ingiustificato ritardo, se sussiste uno dei motivi espressamente previsti, tra cui a titolo esemplificativo e non esaustivo il venir meno della necessità del trattamento rispetto alle finalità, la revoca del consenso su cui si basa il trattamento, opposizione al trattamento nel caso in cui sia basato su interesse legittimo non prevalente, trattamento illecito dei dati, cancellazione per obblighi di legge, dati dei minori trattati in assenza delle condizioni di applicabilità previsto dall'art. 8 del Regolamento;

5. Il Diritto di limitazione del trattamento, ai sensi dell'art. 18 del Regolamento UE, si sostanzia nel diritto a limitare il trattamento illecito, la contestazione dell'esattezza dei dati, l'opposizione dell'interessato e il venir meno del bisogno trattamento da parte del titolare, i dati dell'interessato devono essere trattati solo per la conservazione salvo il consenso dello stesso.
6. Il Diritto alla portabilità dei dati ex art. 20 del Regolamento UE conferiscono all'interessato, nei casi in cui il trattamento si basi sul consenso e sul contratto e sia effettuato con mezzi automatizzati, potrà richiedere di ricevere i propri dati personali in formato strutturato, di uso comune e leggibile da dispositivo automatico, e ha diritto di trasmetterli a un altro titolare.
7. Per Diritto di opposizione, ex art. 21 del Regolamento UE, si intende il diritto dell'interessato di opporsi al trattamento dei propri dati personali, nel caso in cui il trattamento sia basato su interesse legittimo.
8. Il Diritto di non essere sottoposto a processi decisionale automatizzato, ex art. 22 del Regolamento UE, si sostanzia per l'interessato a non essere sottoposto ad una decisione, compresa la profilazione, basata unicamente sul trattamento automatizzato.
9. Il diritto all'obblio di ogni individuo si sostanzia nel diritto ad essere dimenticato per fatti che lo riguardano e che in passato sono stati oggetto di cronaca non più di attualità e rispetto ai quali non vi è un interesse pubblico attuale.
10. L'Ente al venire meno dello scopo rispetto al quale i dati sono stati raccolti, l'interessato ha diritto di ottenere dal Titolare la cancellazione dei dati personali. II Titolare dal trattamento ha l'obbligo di cancellare i dati personali resi pubblici, con la tecnologia disponibile, chiedendo la cancellazione di qualsiasi link, copia o riproduzione dei dati medesimi.

Art. 18 Attività di conciliazione pre-reclamo

1. Fatto salvo il diritto di Reclamo al garante privacy o il ricorso in sede giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi i suoi dati personali ha il diritto, ricorrendo alla modulistica e sulla base della procedura di cui al co.1 dell'art, 17 del presente Regolamento, di richiedere al Responsabile alla protezione dei dati, con istanza motivata, le ragioni della ritenuta violazione e che il comportamento ritenuto lesivo sia dismesso da parte dell'Ente.
2. Il RPD a cui è stata fatta l'istanza informa, prontamente, l'interessato delle circostanze di fatto e delle questioni diritto, nonché dei provvedimenti adottati ai fini della richiesta tutela dello stato, dei tempi e dell'esito della stessa, compresa la possibilità, per il caso di non accoglimento di quanto richiesto perché in violazione di legge, della facoltà di proporre reclamo al Garante o un ricorso in sede giurisdizionale.
3. Nell'istanza deve essere indicato specificamente, anche sulla base del modello appositamente predisposto dall'Ente: l'indicazione dei fatti e delle circostanze su cui si fonda la richiesta; le disposizioni che si presumono violate; le misure richieste da adottare.
4. l'istanza è sottoscritta dall'interessato o, su mandato di questo, da un mandatario con allegata documentazione utile ai fini della sua valutazione e l'eventuale mandato, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica o PEC o telefono.

Art. 19 Trattazione dell'Istanza

1. L'esame dell'istanza è orientato a criteri rapidità e di semplicità delle forme osservate, di celerità ed economicità, anche in riferimento al contraddittorio e il pre-reclamo non comporta alcun contributo spese.
2. la decisione adottata dal RPD è comunicata immediatamente al responsabile del servizio ove la presunta violazione si è verificata e al titolare e avuto l'assenso di questi all'adeguamento è comunicata, senza ritardo all'interessato istante.
3. Ove l'istanza sia irregolare o incompleta ne è data comunicazione all'istante, con l'indicazione delle cause della irregolarità o incompletezza nonché del termine, di regola non superiore a sette giorni, entro cui provvedere alla relativa regolarizzazione, salvo che la stessa sia sanabile o sia possibile interpretarla in ordine all'esercizio del diritto del quale si chiede la tutela.
4. L'istanza, se non sanabile e non tempestivamente regolarizzata è archiviata e può essere esaminata a titolo di segnalazione.

Art.20 Diritto di proporre reclamo al Titolare e al DPO

1. Al termine dell'istruttoria il RPD concludere l'esame dell'istanza archiviandola quando:
   a) la questione prospettata non risulta riconducibile alla protezione dei dati personali;
   b) non sono ravvisati, allo stato degli atti, gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali;
   c) si tratta di una richiesta eccessiva, in particolare per il carattere pretestuoso o ripetitivo anche ai sensi dell'articolo 57 paragrafo 4 del RGPD;
   d) la questione prospettata è stata già decisa con provvedimento del garante.
2. Del provvedimento reso è informato l'interessato istante.

Art. 21 Entrata in vigore – Pubblicità

1.Il presente Regolamento dopo l'approvazione con provvedimento Consiliare sarà pubblicato per 10 giorni consecutivi all'albo on-line dell'Ente ed entra in vigore il quindicesimo giorno successivo. Il presente Regolamento è altresì pubblicato sul sito istituzionale dell'Ente.
2.E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.