REGOLAMENTO

PER LA PROTEZIONE DEI DATI PERSONALI

IN ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679

Approvato con deliberazione Consiglio comunale n. 52 del 22 luglio 2024

Sommario

CAPO I: DISPOSIZIONI GENERALI

ART. 1 Scopo

1. Il presente Regolamento norma la protezione dei dati personali nell'Ente in attuazione del Regolamento (UE) 2016/679 ("GDPR") e del D.Lgs. 196/2003 ("Codice Privacy").
2. Il Regolamento comunale per l'attuazione RGPD definisce le misure procedimentali e le regole di dettaglio per una sua efficace e funzionale applicazione nell'Ente

ART. 2 Definizioni

1. Il presente Regolamento adotta le definizioni di cui all'art.4 GDPR.
2. Ad integrazione delle suddette definizioni, ai fini del presente Regolamento si intende per:

- Responsabile privacy: il soggetto con qualifica dirigenziale (Dirigenti o Segretario Generale) nominato dal Titolare del Trattamento con funzioni di coordinamento e raccordo tra i diversi ruoli previsti nel presente Regolamento;
- Soggetti Designati: i Dirigenti o dipendenti con funzioni apicali che effettuano trattamenti per conto del Titolare, nominati dallo stesso con funzioni di Responsabilità in materia di trattamento dati relativamente al personale assegnato.
- Soggetti Autorizzati: i dipendenti che, sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento, abbiano accesso a dati personali.

CAPO II: ORGANIZZAZIONE PER LA PROTEZIONE DEI DATI PERSONALI

ART. 3 Ruoli

1. La protezione dei dati personali è organizzata nell'Ente sui seguenti ruoli:

- Titolare del trattamento
- Responsabile della Protezione dei Dati personali
- Referente Privacy
- Soggetti Designati
- Soggetti Autorizzati
- Amministratori di Sistema
- Responsabili esterni del trattamento
- Contitolari del trattamento

ART. 4 Titolare del trattamento

1. Ai sensi dell'articolo 4 comma 7 del GDPR, il Titolare del trattamento ("Titolare") è la persona giuridica dell'Ente, rappresentata dal Sindaco pro tempore in qualità di legale rappresentante dell'Ente.
2. Ai sensi dell'articolo 2-quaterdecies del Codice Privacy, il legale rappresentante può designare come propri Delegati dirigenti di ciascuna area specificando nell'atto di designazione i compiti relativi alla protezione dei dati personali che intende delegare.

ART. 5 Responsabile della Protezione dei Dati personali

1. Ai sensi dell'articolo 37 del GDPR e seguenti, Il Titolare designa un Responsabile della Protezione dei Dati personali (RPD) e ne dà comunicazione al Garante, anche esterno in possesso di competenze specifiche in materia.
2. Il Responsabile Privacy coordina le relazioni dell'Ente col RPD. I Soggetti Designati si relazionano con il RPD secondo le modalità definite dal Responsabile Privacy, tenendo aggiornato il Responsabile Privacy.
3. Gli Incaricati non tengono relazioni dirette col RPD, se non per la gestione di casi particolari.

ART. 6 Referente Privacy

1. Il Titolare designa un Referente Privacy dell'Ente ("Referente Privacy"), con compiti di coordinamento e controllo operativi relativamente alla protezione dei dati nell'Ente.
2. Il Referente Privacy:
   - collabora con i dirigenti dell'Ente e in particolare con gli uffici staf e ufficio transizione digitale dell'Ente per la piena attuazione del GDPR in conformità al presente Regolamento;
   - predispone in collaborazione con i Dirigenti i modelli previsti dal presente Regolamento;
   - verifica con cadenza annuale l'effettiva attuazione di quanto previsto dal previsto Regolamento, riferendone l'esito al Titolare;
   - funge da riferimento per le relazioni col RPD e monitora l'attuazione delle sue raccomandazioni;
   - informa l'Ente sull'evoluzione normativa che ha impatti sulla protezione dei dati personali e propone modifiche al presente Regolamento;
   - svolge tutti gli altri compiti assegnatigli dal presente Regolamento.

ART. 7 Soggetti Designati

1. Ai sensi dell'art. 2-quaterdecies comma 1 del Codice Privacy, Il Titolare attribuisce alle figure apicali coincidenti con i Dirigenti di Area la responsabilità di applicare il presente Regolamento nell'ambito organizzativo di cui sono a capo.
2. La designazione specifica l'ambito di responsabilità del Soggetto Designato ed è valida fino a nuova designazione per il medesimo ambito.
3. Con la designazione, il Titolare autorizza in via generale il Soggetto Designato a ricorrere a Responsabili esterni del trattamento, così che il Soggetto Designato possa sottoscrivere contratti con soggetti esterni che trattano dati personali per conto dell'Ente.
4. In collaborazione con il Servizio Staff, il Referente Privacy predispone il modello per la designazione dei Soggetti Designati e segnala la necessità di nuove designazioni.

ART. 8 Soggetti Autorizzati

1. Ai sensi dell'articolo 29 del GDPR e dell'articolo 2-quaterdecies comma 2 del Codice Privacy, sono Soggetti Autorizzati i dipendenti, i collaboratori ed i volontari che trattano dati personali sotto l'autorità del Titolare o di un Soggetto Designato.
2. L'assegnazione di un soggetto ad una unità organizzativa lo autorizza, senza necessità di altri atti da parte del Titolare, a trattare i dati personali necessari ai procedimenti svolti in quell'unità organizzativa e limitatamente alle proprie mansioni. L'assegnazione del soggetto ad una o più unità organizzative è documentata dal PEG e dall'allegato al PIAO relativo al personale in servizio per area.
3. Il Responsabile interno predispone e distribuisce istruzioni specifiche ai propri Incaricati, ne verifica l'esecuzione e identifica ulteriori necessità di istruzione.
4. Ai sensi dell'articolo 29 del GDPR, il Titolare provvede all'istruzione del Soggetto Autorizzato mediante corsi inseriti nel Piano di Formazione dell'Ente, il disciplinare all'uso dei sistemi informatici predisposto dal Servizio Informatico, il manuale di gestione documentale, il codice di comportamento e specifiche istruzioni dell'unità organizzativa cui il Soggetto è assegnato.

ART. 9 Amministratori di Sistema

1. Il Titolare ricorre ad uno o più Amministratori di Sistema, interni o esterni all'Ente, i cui compiti sono definiti dal Provvedimento del Garante della Protezione dei Dati Personali ("Garante") del 27 novembre 2008 e seguenti.
2. Il Titolare o suo delegato designa per iscritto gli Amministratori di Sistema, definendone l'ambito di responsabilità, utilizzando modelli predisposti dal Responsabile Privacy o modelli equivalenti proposti dai soggetti esterni.
3. Il Responsabile Privacy custodisce copia delle designazioni effettuate.

ART. 10 Responsabili esterni del trattamento

1. Ai sensi dell'articolo 28 del GDPR, il Titolare o il Soggetto Designato designa, come Responsabili del trattamento i soggetti esterni all'Ente, che trattano dati personali per conto del Titolare.
2. In collaborazione col Referente Privacy, il area staff predispone modelli di clausole contrattuali e di atti separati per la designazione dei Responsabili esterni.
3. Con la collaborazione dei Soggetti Designati, il Referente Privacy tiene un elenco aggiornato dei fornitori pro tempore, che consente di conoscere nominativamente i destinatari dei dati personali indicati come categorie nei Registri delle attività di trattamento di cui all'articolo 12 e nelle informative di cui all'articolo 19.

ART. 11 Collaborazioni con altri Enti

1. Laddove la comunicazione di dati personali tra l'Ente ed altri enti pubblici non ricada nei casi previsti dall'articolo 2-ter del Codice Privacy, tale comunicazione è regolata da Convenzioni, che possono configurarsi come:
   - un accordo di contitolarità ai sensi dell'articolo 26 del GPDR, qualora gli Enti definiscano congiuntamente finalità e mezzi del trattamento, oppure
   - un contratto o atto giuridico equivalente ai sensi dell'articolo 28 del GPDR, qualora un Ente (Responsabile) svolga trattamenti di dati personali per conto di un altro Ente (Titolare).
2. Se la Convenzione non contiene le informazioni richieste dal GDPR, l'Ente propone agli altri Enti appositi accordi integrativi, col supporto del RPD.
3. Il Referente Privacy supporta il Titolare ed i Soggetti Designati della casistica applicabile alle diverse collaborazioni dell'Ente e nella predisposizione degli eventuali accordi integrativi.

CAPO III: MISURE PER LA PROTEZIONE DEI DATI PERSONALI

ART. 12 Registri delle attività di trattamento

1. Ai sensi dell'articolo 30 del GDPR, il Titolare tiene un Registro delle attività di trattamento svolte sotto la propria responsabilità ("Registro del Titolare").
2. Il Registro del Titolare è approvato da la Giunta Comunale e l'atto di approvazione è pubblicato in Amministrazione Trasparente, mentre il Registro non viene pubblicato.
3. Il Referente Privacy predispone lo schema del Registro, ne aggiorna il contenuto con la collaborazione dei Dirigenti, dei Soggetti Designati, lo verifica annualmente e lo mette a disposizione del RPD e del Garante.

4. Se l'Ente svolge attività come Responsabile del trattamento per conto di altri Titolari, viene istituito anche il Registro delle attività del Responsabile ("Registro del Responsabile"), con caratteristiche e modalità analoghe a quelle previste per il Registro del Titolare.

ART. 13 Valutazione del rischio dei trattamenti

1. Ogni Soggetto Designato provvede alla valutazione del rischio delle proprie attività di trattamento descritte nei Registri di cui all'articolo 0.
2. La valutazione del rischio è svolta secondo una metodologia proposta dal Referente Privacy e validata dal RPD. Il risultato della valutazione è riportato dal Referente Privacy nel Registro delle attività o in uno specifico documento, fornendo così al Titolare elementi oggettivi ed uniformi per l'identificazione dei trattamenti che comportano maggiori rischi per gli interessati e per la definizione delle priorità di intervento per mitigarli.
3. Il Referente Privacy segnala ai Soggetti Designati i trattamenti per cui è necessaria la Valutazione di Impatto ai sensi dell'articolo 35 del GDPR. La Valutazione di Impatto è curata dal Soggetto Designato nel cui ambito ricade il trattamento che la richiede, è validata dal RPD ed approvata dal Titolare.
4. Alla luce del risultato della Valutazione di Impatto, il Referente Privacy segnala al Titolare l'eventuale necessità di Consultazione preventiva di cui all'articolo 36 del GDPR.

ART. 14 Valutazione 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 RGDP, 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, RGDP.
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, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono indicativamente i seguenti:
   a. valutazione o assegnazione di punteggi, 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. 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;

c. trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;

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

Il Titolare deve consultarsi con il 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.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare o suo delegato per lo svolgimento della DPIA.

5. 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.

Il RPD fornisce, 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 RGPD;

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

— se il trattamento non può comportare un rischio elevato per i diritti e le

libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;

— se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;

— se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;

— 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.

7. I processi relativi all'adozione della DPIA saranno concordati con il DPO.

ART. 15 Sicurezza Informatica

1. La sicurezza informatica nell'Ente è assicurata dal Responsabile Servizi Informatici, qualora non nominato coincide con il Dirigente di Riferimento.

ART. 16 Sicurezza fisica

1. Ciascun Responsabile interno assicura, in collaborazione col Responsabile Privacy, l'adeguatezza dei luoghi di lavoro e degli archivi ai fini della protezione dei dati personali, con particolare attenzione ai rischi di accesso fisico non autorizzato ad uffici, archivi, stampe, chiavi, server, apparati di rete e quadri elettrici.

ART. 17 Trattamenti non informatizzati

1. Nell'ambito di propria responsabilità, ogni Soggetto Designato:
    - verifica che le modalità operative dei trattamenti non informatizzati offrano un livello adeguato di protezione dei dati personali, con particolare attenzione all'accesso fisico ad uffici, archivi e stampanti, alla presenza di documenti contenenti dati personali negli spazi comuni (corridoi, sale ristoro), al rischio di ascolto di conversazioni riservate e ad ogni altra situazione che possa comportare rischi di violazioni di dati personali
    - segnala al Titolare ed al Referente Privacy le situazioni a rischio rilevate e propone misure tecniche ed organizzative per ridurre il rischio
    - provvede tempestivamente all'attuazione delle misure approvate e finanziate.

- definisce le regole di accesso controllato e tracciato agli archivi centrali e le regole di scarto della documentazione cartacea.

CAPO IV: RELAZIONI CON GLI INTERESSATI

ART. 18 Informative

1. Il Referente Privacy predispone i modelli delle informative di cui all'articolo 13 del GDPR, definisce le modalità di collegamento tra informative e modulistica e verifica che Informative e moduli pubblicati siano coerenti coi modelli.
2. Ogni Soggetto Designato predispone per i propri servizi le Informative e le collega alla modulistica.

ART. 19 Diritti degli interessati

1. I dirigenti per quanto di competenza, definiscono le modalità con cui gli interessati possono far valere i diritti di cui all'articolo 15 del GDPR e seguenti e cura la trasmissione delle richieste degli interessati al Referente Privacy.
2. Il Referente Privacy cura la risposta alle richieste pervenute, in collaborazioni coi Soggetti Designati.

CAPO V: GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

ART. 20 Segnalazioni di potenziali violazioni

1. Il Responsabile Privacy predispone sul sito istituzionale le istruzioni per la segnalazione di potenziali violazioni dei dati personali trattati dal Titolare e, sulla intranet dell'Ente, analoghe istruzioni rivolte agli Incaricati.
2. L'Incaricato che viene a conoscenza di una possibile violazione di dati personali è tenuto a metterne tempestivamente a conoscenza il Titolare attraverso le modalità pubblicate sulla intranet o, in casi di particolare urgenza, segnalandola direttamente al proprio responsabile o, in sua assenza, ad un altro responsabile organizzativo apicale.

ART. 21 Valutazione della segnalazione

1. La valutazione della segnalazione è eseguita nel rispetto dell'art. 33 GDPR.
2. La valutazione della segnalazione è responsabilità del Dirigente di competenza, col supporto del Responsabile Privacy, di eventuali altri uffici dell'Ente in grado di fornire elementi utili alla valutazione e dei Responsabili esterni coinvolti nel trattamento.
3. In caso di indisponibilità del Dirigente o qualora la segnalazione riguardi più ambiti, la valutazione è eseguita dal Responsabile Privacy.
4. La valutazione deve concludersi in tempo utile a consentire l'eventuale notifica al Garante entro le 72 ore dal momento dell'avvenuta segnalazione.

ART. 22 Gestione delle violazioni

1. Ogni dipendente dell'Ente deve segnalare tempestivamente al Soggetto Designato dell'unità organizzativa cui è assegnato le situazioni di potenziale violazione di dati personali, fornendo ogni dettaglio utile alla valutazione. In assenza del Soggetto Designato, il dipendente la segnala al referente privacy.
2. Se la segnalazione non riguarda il proprio ambito, il Soggetto Designato interpellato inoltra senza indugio la segnalazione al Soggetto Designato nel cui ambito è presumibilmente avvenuta la violazione. Se la segnalazione riguarda generalmente i sistemi informatici, deve essere inoltrata al responsabile del Servizio Informatico. Il soggetto così identificato (Soggetto Designato o Responsabile dell'Servizio Informatico) assume il ruolo di Responsabile della Segnalazione.
3. Con la collaborazione del Referente Privacy e del Servizio Informatico, il Responsabile della Segnalazione valuta se sia effettivamente avvenuta una violazione di dati personali e, in caso affermativo, valuta il rischio per gli interessati ai sensi e nel rispetto dei vincoli temporali dell'articolo 33 del GDPR:
   - Se il rischio per gli interessati è valutato "improbabile", la segnalazione viene chiusa. Il Referente Privacy può opporsi a tale valutazione rivolgendosi al legale rappresentante o suo Delegato
   - Se il rischio è valutato "probabile", il Responsabile della Segnalazione attiva immediatamente le prime misure tecniche ed organizzative in grado di mitigare il rischio. Sentito il RPD, il Referente Privacy provvede alla notifica al Garante, firmata dal legale rappresentante dell'Ente.
   - Se il rischio è valutato "elevato", il Referente Privacy provvede alla comunicazione agli interessati ai sensi dell'articolo 35 del GDPR.
4. Ai sensi dell'articolo 33 comma 5 del GDPR, è istituito il Registro delle Violazioni per la documentazione delle attività svolte nella gestione delle violazioni. Il Referente Privacy vi riporta sinteticamente i casi gestiti e lo mette a disposizione del RPD e del Garante.

ART. 23 Misure di contenimento

1. Se la valutazione conferma l'avvenuta violazione di dati personali, il Responsabile interno o il Responsabile Privacy ordina immediatamente misure tecniche ed organizzative atte a contenere il rischio per le persone fisiche.

ART. 24 Notifica al Garante

1. Se la valutazione della segnalazione si conclude confermando l'avvenuta violazione di dati personali, e valutando che sia "probabile" che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, il Responsabile Privacy - sentito il RPD - predispone la notifica al Garante sottoponendola alla firma del legale rappresentante dell'Ente o suo delegato e provvedendo all'inoltro, secondo le modalità definite dal Garante stesso.

ART. 25 Comunicazione agli Interessati

1. Se la valutazione della segnalazione si conclude confermando l'avvenuta violazione di dati personali, e valutando che il rischio per i diritti e le libertà delle persone fisiche sia "elevato", il Responsabile Privacy – sentito il RPD - predispone la comunicazione agli Interessati, con le modalità definite dall'art.34 GDPR.
2. L'effettiva esecuzione delle comunicazioni agli Interessati deve tener conto delle avvertenze dei Considerando 86 e 88 del GDPR.

ART. 26 Registro delle Violazioni

1. Ai sensi dell'art.33.5 GDPR, il Responsabile Privacy predispone, aggiorna e custodisce il Registro delle Violazioni, in cui vengono annotate le informazioni relative alle violazioni dei dati personali.
2. Anche le segnalazioni per le quali la valutazione si conclude escludendo una violazione dei dati personali sono sinteticamente riportate nel Registro delle Violazioni.
3. Il Registro delle Violazioni è messo a disposizione su richiesta al RPD ed al Garante.

ART. 27 Modello Organizzativo

1. Ai fini della gestione di dettaglio del modello organizzativo si demanda alla Giunta comunale, l'approvazione di modulistiche o direttive.

ART. 28 Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

ART. 29 Norma finale

1. Il presente regolamento entra in vigore dopo intervenuta esecutività della deliberazione consiliare di approvazione. Si considerano abrogate tutte le precedenti norma in contrasto.