



Comune di Settimo Torinese
Modello organizzativo
in materia di protezione dei dati personali

INDICE

1. TITOLARE DEL TRATTAMENTO	3
2. RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI	3
3. REFERENTE PRIVACY	4
4. SOGGETTI DESIGNATI	4
5. SOGGETTI AUTORIZZATI	5
6. RESPONSABILI ESTERNI DEL TRATTAMENTO	6
7. COLLABORAZIONI CON ALTRI ENTI	6
8. REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO	6
9. VALUTAZIONE DEL RISCHIO DEI TRATTAMENTI	7
10. AMMINISTRATORI DI SISTEMA E TRATTAMENTI INFORMATIZZATI	7
11. TRATTAMENTI NON INFORMATIZZATI	7
12. INFORMATIVE	7
13. DIRITTI DEGLI INTERESSATI	8
14. GESTIONE DELLE VIOLAZIONI	8

Il presente documento ha per oggetto misure procedurali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento (UE) 2016/679 ("GDPR") e del D.Lgs. 196/2003 ("Codice Privacy") ed in particolare:

- a) individua i compiti del Titolare e dei Responsabili, nonché degli autorizzati al trattamento dei dati personali esistenti e gestiti presso gli uffici comunali;
- b) disciplina il trattamento dei dati personali effettuato dall'Amministrazione comunale nello svolgimento dei propri compiti istituzionali.

I trattamenti sono compiuti dal Comune di Settimo Torinese per le seguenti finalità:

- a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
- b) l'adempimento di un obbligo legale al quale è soggetto il Comune;
- c) l'esecuzione di un contratto con soggetti interessati o per la conclusione dello stesso;
- d) per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;
- e) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Rientrano nelle finalità di cui al comma 1 lett. a) i trattamenti compiuti per:

- a) l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio;
- b) la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
- c) l'esercizio di ulteriori funzioni amministrative affidate al Comune per servizi di competenza statale o regionale in base alla vigente legislazione, ovvero per altri servizi in base a convenzione;
- d) la tutela in giudizio del Comune.

1. Titolare del trattamento

Ai sensi dell'articolo 4 comma 7 del GDPR, il Titolare del trattamento è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".

Il Comune di Settimo Torinese, rappresentato legalmente dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali compiuto per lo svolgimento delle funzioni istituzionali dalle proprie articolazioni organizzative o da parte di terzi per suo conto.

Ai sensi dell'articolo 2-quaterdecies del Codice Privacy, il legale rappresentante può designare quali delegati il Segretario Generale e i Dirigenti, specificando nell'atto di designazione i compiti relativi alla protezione dei dati personali che intende delegare.

Le funzioni di Titolare del trattamento sono esercitate da ciascun Dirigente nel rispettivo ambito di competenza, in conformità all'assetto organizzativo del Comune e alle disposizioni del presente documento.

2. Responsabile della Protezione dei Dati personali

Ai sensi dell'articolo 37 e seguenti del GDPR, Il Titolare designa un Responsabile della Protezione dei Dati personali (RPD/DPO) e ne dà comunicazione al Garante.

Il RPD assolve i compiti previsti dall'art. 39 del GDPR e gli eventuali altri compiti affidati allo stesso dal Sindaco.

Il Comune garantisce al RPD, per l'esecuzione di compiti ad esso affidati, l'autonomia e le risorse necessarie per assolverli.

Il RPD propone, in raccordo con il Referente Privacy, un ordine di priorità nell'attività da svolgere, ovvero un piano annuale di attività, incentrandola sulle aree che presentano maggiori rischi in termini di protezione dei dati.

Il RPD può convocare incontri con i dirigenti e i dipendenti per l'esecuzione dei propri compiti di informazione, consulenza, sorveglianza e consultazione e può altresì organizzare specifiche giornate di formazione.

Il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. Referente Privacy

Il Titolare designa un Referente Privacy con compiti di coordinamento e controllo operativi relativamente alla protezione dei dati nell'Ente. Per supportare l'attività del Referente è stato istituito l'Ufficio Privacy.

Il Referente Privacy:

- collabora con i servizi e gli uffici dell'Ente per la piena attuazione del GDPR in conformità al presente modello organizzativo
- predispone i modelli previsti dal presente documento (nomina soggetti Designati, nomina soggetti autorizzati al trattamento dati personali, nomina responsabile esterno del trattamento art. 28 GDPR, modello registro dei trattamenti e registro delle violazioni, modelli delle informative di cui all'articolo 13 del GDPR)
- verifica con cadenza annuale l'effettiva attuazione di quanto previsto dal Regolamento GDPR, riferendone l'esito al Titolare
- funge da riferimento per le relazioni col RPD e monitora l'attuazione delle sue raccomandazioni
- informa l'Amministrazione sull'evoluzione normativa che ha impatti sulla protezione dei dati personali e propone modifiche al presente documento
- svolge tutti gli altri compiti assegnatigli dal presente modello organizzativo

4. Soggetti Designati

Ai sensi dell'art. 2-quaterdecies comma 1 del D.Lgs 196/2003 (Codice Privacy), Il Titolare attribuisce alle figure apicali di Settore la responsabilità di applicare il presente regolamento nell'ambito organizzativo di cui sono a capo.

La designazione specifica l'ambito di responsabilità del Soggetto Designato ed è valida fino a nuova designazione.

Con la designazione, il Titolare autorizza in via generale il Soggetto Designato a ricorrere a Responsabili esterni del trattamento.

Ai soggetti Designati vengono attribuiti i seguenti compiti specifici:

- a) adottare e sottoscrivere tutti gli atti amministrativi, negoziali o unilaterali, nell'ambito delle attribuzioni previste dagli articoli 107/109 del D.Lgs 18 agosto 2000 n. 267;
- b) assicurare l'esattezza degli adempimenti previsti dagli articoli 37, 38 e 39 in materia di responsabile della protezione dei dati;
- c) sottoscrivere contratti e/o adottare e sottoscrivere atti e provvedimenti per la disciplina dei rapporti con i responsabili del trattamento (art. 28 GDPR);
- d) designare gli autorizzati al trattamento, sottoscrivendo i relativi atti di autorizzazione;
- e) curare la stesura del registro dei trattamenti (articolo 30 GDPR);
- f) curare e sottoscrivere atti e provvedimenti nei confronti degli interessati del trattamento (articoli 12 e seguenti GDPR).

L'Ufficio Privacy predispone e aggiorna il modello per la designazione dei Soggetti Designati.

5. Soggetti Autorizzati

Il Dirigente procede, per il tramite dell'Ufficio Privacy, a designare all'interno della propria struttura operativa il personale dipendente autorizzato per l'espletamento di tutte le operazioni di trattamento dei dati.

La designazione è fatta con atto scritto nel quale sono specificati i compiti affidati agli autorizzati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati.

Gli Autorizzati effettuano tutte le operazioni di trattamento dei dati nel rispetto delle istruzioni e direttive impartite dal proprio Dirigente che prevedono di:

- a) accedere solo ai dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;
- b) trattare i dati personali di cui si viene a conoscenza per l'espletamento delle proprie funzioni, in modo lecito e corretto, nel rispetto delle norme di legge, dello Statuto e dei Regolamenti che disciplinano le attività del Comune;
- c) verificare costantemente i dati, il loro aggiornamento, la loro completezza e pertinenza;
- d) custodire con cura atti e documenti contenenti dati personali ricevuti in consegna per adempiere ai compiti assegnati e restituirli al termine delle operazioni affidate;
- e) comunicare i dati personali trattati solo previa autorizzazione;

f) osservare scrupolosamente le misure di sicurezza predisposte;

g) osservare, anche in seguito a modifica, trasferimento e/o cessazione del rapporto di lavoro, gli obblighi relativi alla riservatezza e alla comunicazione.

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.

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, il manuale di gestione documentale, il codice di comportamento, circolari interne e specifiche istruzioni dell'unità organizzativa cui il Soggetto è assegnato.

6. Responsabili esterni del trattamento

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.

L'Ufficio Privacy, su indicazioni del Referente, predispone e aggiorna il modello di nomina a Responsabile esterno del trattamento dei dati personali.

Un elenco aggiornato dei fornitori pro tempore, che consente di conoscere nominativamente i Responsabili esterni, è reperibile nel Registro delle attività di trattamento.

7. Collaborazioni con altri Enti

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).

Se la Convenzione non contiene le informazioni richieste dal GDPR, l'Ente propone agli altri Enti appositi accordi integrativi, col supporto del RPD.

Il Referente Privacy supporta il Titolare ed i Soggetti Designati in merito alla casistica applicabile alle diverse collaborazioni dell'Ente e nella predisposizione degli eventuali accordi integrativi.

8. Registri delle attività di trattamento

Ai sensi dell'articolo 30 del GDPR, il Titolare tiene un Registro delle attività di trattamento svolte sotto la propria responsabilità ("Registro del Titolare").

L'Ufficio Privacy, su indicazioni del Referente, predispone lo schema del Registro, ne aggiorna il contenuto con la collaborazione dei Soggetti Designati, lo verifica annualmente e lo mette a disposizione del RPD e del Garante.

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.

9. Valutazione del rischio dei trattamenti

Ogni Soggetto Designato provvede alla valutazione del rischio delle proprie attività di trattamento descritte nei Registri di cui all'articolo 8.

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.

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.

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.

10. Amministratori di Sistema e trattamenti informatizzati

La società SAT scarl, società in house che eroga il servizio di gestione e sviluppo dei sistemi informativi dell'Ente, designa gli Amministratori di Sistema con i compiti definiti dal Provvedimento del Garante del 27 novembre 2008 e s.m.i. (nota acquisita agli atti con prot. n. 47801/2023 e successiva nota di aggiornamento prot. n. 61571/2025).

Le designazioni specificano l'ambito di responsabilità del singolo Amministratore di Sistema in termini di servizi e/o sistemi informatici amministrati.

11. Trattamenti non informatizzati

Nell'ambito della 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.

Il Responsabile della gestione documentale dell'ente definisce le regole di accesso controllato e tracciato agli archivi centrali e le regole di scarto della documentazione cartacea.

12. Informative

L'Ufficio Privacy predispose i modelli delle informative di cui all'articolo 13 del GDPR su indicazioni del Referente Privacy.

Ogni Soggetto Designato dà indicazioni ai propri servizi di predisporre le informative e verifica che informative e moduli pubblicati siano coerenti con i modelli.

13. Diritti degli interessati

Il Referente Privacy definisce le modalità con cui gli interessati possono far valere i diritti ai sensi dell'articolo 15 e seguenti del Regolamento UE 2016/679 (GDPR) e cura la risposta alle richieste pervenute, in collaborazione con i Soggetti Designati.

14. Gestione delle violazioni

Con determinazioni n. 362/2020 e n. 466/2020 il Comune ha approvato la procedura da adottare in caso di violazione dei dati personali (data breach).

Ogni dipendente dell'Ente deve segnalare tempestivamente al Dirigente/Soggetto Designato dell'unità organizzativa cui è assegnato le situazioni di potenziale violazione di dati personali, fornendo ogni dettaglio utile alla valutazione. In sua assenza, il dipendente la segnala al Segretario Generale o al Dirigente del Settore Servizi Generali o all'Ufficio Privacy.

Con la collaborazione del Referente Privacy e del servizio informatico, il Dirigente interessato 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 e il Referente Privacy la fa annotare nel Registro delle violazioni.
- se il rischio è valutato "probabile", il Dirigente interessato 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 o suo delegato designato.

- se il rischio è valutato “elevato”, il Referente Privacy provvede alla comunicazione agli interessati ai sensi dell’articolo 35 del GDPR, sentito il RPD.

Ai sensi dell’articolo 33 comma 5 del GDPR, il Comune ha istituito il Registro delle Violazioni per la documentazione delle attività svolte nella gestione delle violazioni. L’Ufficio Privacy vi riporta sinteticamente i casi gestiti e lo mette a disposizione del RPD e del Garante.