COMUNE ROSIGNANO MARITTIMO

REGOLAMENTO PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Approvato con deliberazione del Consiglio Comunale n. ___ del _____

INDICE

TITOLO I - NORME INTRODUTTIVE

ART. 1	Oggetto	pag.	4
ART. 2	Definizioni	pag.	4
ART. 3	Finalità del trattamento	pag.	4

TITOLO II - ORGANIZZAZIONE DEL TITOLARE

ART. 4	Titolare del trattamento	pag.	5
ART. 5	Compiti dei Responsabili interni designati dal Titolare	pag.	5
ART. 6	Ruolo della Unità Organizzativa Segretariato	pag.	6
ART. 7	Compiti della Unità Organizzativa Sistemi informativi e Innovazione tecnologica	pag.	6
ART. 8	Responsabile esterno del trattamento	pag.	7
ART. 9	Incaricati al trattamento	pag.	7
ART. 10	Amministratori di sistema	pag.	8
ART. 11	Responsabile della protezione dei dati (DPO)	pag.	8
ART. 12	Attività di monitoraggio	pag.	9

TITOLO III - TRATTAMENTO DEI DATI PERSONALI

ART. 13	Registro delle attività di trattamento	pag.	9
ART. 14	Consenso dell'interessato.	pag.	9
ART. 15	Informativa	pag.	9
ART. 16	Diritti dell'interessato	pag.	10
ART. 17	Sicurezza del trattamento	pag.	10
ART. 18	Durata del trattamento	pag.	10
ART. 19	Valutazione di impatto	pag.	11
ART. 20	Violazione dei dati personali	pag.	11
ART. 21	Formazione del personale	pag.	11
ART. 22	Trattamento dei dati personali da parte di Amministratori	pag.	12
ART. 23	Comunicazione e diffusione dei dati personali comuni	pag.	12
ART. 24	Norma finale	pag.	12

TITOLO I

NORME INTRODUTTIVE

ART. 1 - Oggetto

1. Il presente Regolamento ha ad oggetto le modalità di attuazione delle disposizioni del Regolamento europeo n. 679 del 27 aprile 2016 (di seguito "GDPR") e del "Codice in materia di protezione dei dati personali", di seguito denominato "Codice", approvato con D.Lgs. 30 giugno 2003 n.196, come modificato dal D.Lgs 101 del 10 agosto 2018 ed in particolare:

a) disciplina il trattamento dei dati personali effettuato dal Comune di Rosignano Marittimo nello svolgimento dei propri compiti istituzionali;
b) individua i compiti del Titolare e dei Responsabili, nonché degli incaricati del trattamento dei dati personali esistenti e gestiti presso gli uffici comunali.

ART. 2 - Definizioni

1. Ai fini del presente Regolamento si intende per:

- «titolare del trattamento»: il Comune di Rosignano Marittimo quale entità organizzativa complessa;
- «responsabili interni»: i singoli dirigenti e/o funzionari del Comune di Rosignano Marittimo nei ~~per i~~ rispettivi ambiti di competenza designati dal Titolare;
- «incaricati»: i soggetti interni designati ed autorizzati con nomina scritta per competenza da parte del responsabile interno al trattamento dei dati personali;
- «responsabile esterno del trattamento»: la persona fisica o giuridica, o altro organismo, estraneo al Comune di Rosignano Marittimo, che tratta dati personali per conto del titolare del trattamento;
- «sub-responsabile esterno del trattamento»: la persona fisica o giuridica o altro organismo, estraneo al Comune di Rosignano Marittimo, a cui fa ricorso il responsabile esterno del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;
- «interessato»: la persona fisica alla quale si riferiscono i dati;
- «amministratore di sistema»: la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi i gestione delle banche dati informatiche, i sistemi software complessi, le reti locali e gli apparati di sicurezza;
- «responsabile della protezione dei dati (RPD/DPO)»: il soggetto che svolge i compiti di cui all'art. 39 del GDPR e/o gli ulteriori compiti affidati dal titolare del trattamento.
- "data breach": una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. Per le altre definizioni si rinvia all'art. 4 del GDPR.

Art. 3 - Finalità del trattamento

1. I trattamenti sono compiuti dal Comune di Rosignano Marittimo per il conseguimento di finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (art. 5, lett. b, GDPR), in particolare per:

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 di Rosignano Marittimo;
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 previa fornitura di puntuale informativa;

2. 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, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
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 di Rosignano Marittimo 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 di Rosignano Marittimo.

TITOLO II

ORGANIZZAZIONE DEL TITOLARE

ART. 4 - Titolare del trattamento

1. Il Comune di Rosignano Marittimo, rappresentato ai fini previsti dal Sindaco pro-tempore, è il Titolare del trattamento dei dati personali compiuto per lo svolgimento delle relative funzioni istituzionali dalle proprie articolazioni organizzative o da parte di terzi per suo conto.

2. Il Titolare definisce, fin dalla fase di progettazione, le necessarie misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato in modo conforme al GDPR e al Codice privacy.

3. Gli interventi necessari per l'attuazione delle misure di cui al precedente comma sono inseriti nell'ambito degli strumenti di programmazione e operativi quali il Piano triennale dell'Informatica.

4. Il titolare del trattamento, secondo quanto previsto dal D.Lgs. n. 196/2003 art.2 quaterdecies, comma 1 e 2 e ss.mm.ii., designa con apposito decreto i responsabili interni del trattamento che, in conformità all'assetto organizzativo del Comune di Rosignano Marittimo e nel rispettivo ambito di competenza, danno attuazione alle disposizioni del GDPR, di tutte le norme vigenti relative al trattamento dei dati personali, alle indicazioni del Garante della Privacy e del presente regolamento.

5. Laddove il Comune di Rosignano Marittimo determini finalità e mezzi di un trattamento di dati personali congiuntamente ad altro soggetto, pubblico o privato, tale soggetto diviene contitolare del trattamento, secondo quanto previsto dall'art. 26 del GDPR.

Art 5 - Compiti dei Responsabili interni designati dal Titolare

1. I Responsabili interni designati dal Titolare al trattamento dei dati personali, nell'ambito delle strutture organizzative cui sono preposti, assicurano il rispetto degli obblighi normativi previsti in capo al Titolare del trattamento in relazione ai trattamenti di loro competenza.

2. Tali soggetti provvedono in particolare a:

a) censire e monitorare costantemente le singole attività di trattamento dei dati personali facenti capo alla Unità Organizzativa/Servizio e ai soggetti designati ed autorizzati che non siano direttamente inseriti nell'organico delle Unità Organizzative/Servizi del Comune di Rosignano Marittimo;
b) fornire prontamente ogni elemento necessario alla regolare tenuta del Registro unico delle attività di trattamento predisposto dal Comune di Rosignano Marittimo ai sensi dell'art. 13 del presente regolamento al fine di consentire il costante aggiornamento dello stesso;

c) designare con atto scritto gli incaricati al trattamento dei dati personali con le modalità di cui all'art. 9 del presente regolamento;
d) vigilare sulle attività dei soggetti incaricati di cui al precedente punto e garantirne una adeguata formazione nell'ambito delle iniziative predisposte dal Comune di Rosignano Marittimo e dal DPO;
e) disciplinare il rapporto con eventuali Responsabili esterni del Trattamento e procedere per iscritto alla loro nomina secondo le modalità previste dall'art. 8 del presente Regolamento;
f) prima di procedere al trattamento, effettuare l'analisi del rischio e, ove necessario, la valutazione di impatto ai sensi dell'art. 35 del GDPR e dell'art. 19 del presente regolamento;
g) provvedere, in relazione alla natura dei dati e alle specifiche caratteristiche del trattamento, a monitorare l'adeguatezza delle misure di sicurezza adottate;
h) informare tempestivamente il titolare per la notifica al Garante della violazione dei dati personali (data breach) e provvedere alla comunicazione della violazione agli interessati dandone informativa alla Unità Organizzativa Segretariato e al DPO/RPD ai sensi dell'art. 20 del presente regolamento;
i) collaborare con il DPO/RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
j) garantire l'esercizio dei diritti degli interessati previsti agli articoli da 15 a 18 e da 20 a 22 del GDPR e dar corso alle relative richieste;
k) predisporre le informative e curarne il costante aggiornamento.

3. Ciascun Responsabile interno tiene il registro dei trattamenti delle U.O./Servizi che afferiscono al settore di propria competenza e fornisce prontamente ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico di cui all'art. 13 del presente regolamento.

4. Ciascun Responsabile interno predispone un elenco dei responsabili esterni del trattamento che comunica alla U.O. Segretariato e lo aggiorna periodicamente.

5. Qualora all'interno del Comune di Rosignano Marittimo vi siano banche dati o applicativi condivisi tra più Unità Organizzative, le decisioni in ordine agli adempimenti previsti dal GDPR e dal Codice spettano al Responsabile interno a cui competono le funzioni ed attività per il cui svolgimento è stato sviluppato il software o la banca dati informatica.

Art. 6 – Ruolo dell'Unità Organizzativa Segretariato

1. Alla Unità Organizzativa Segretariato compete l'adozione delle misure volte a garantire l'uniformità di applicazione del GDPR all'interno dell'Ente. Tale Unità Organizzativa si avvale di un ufficio amministrativo in materia di privacy che fornisce adeguato supporto alle altre strutture, anche predisponendo l'opportuna modulistica.

2. L'Unità Organizzativa Segretariato raccoglie i registri di competenza dei Responsabili interni al fine di formare il Registro unico dei trattamenti di cui all'art. 13 del presente regolamento, approvandone periodicamente gli aggiornamenti e disponendo eventualmente modalità operative per l'organizzazione dello stesso.

3. La Unità Organizzativa Segretariato collabora e fornisce adeguato supporto al DPO/RPD.

Art. 7 - Compiti dell'Unità Organizzativa Sistemi informativi e Innovazione tecnologica

1. Alla Unità Organizzativa Sistemi informativi e Innovazione tecnologica competono lo sviluppo e la gestione delle applicazioni e dei sistemi informatici dell'Ente. Nello svolgimento di tali attività, alla U.O. Sistemi informativi e Innovazione tecnologica spettano i seguenti compiti:
a) provvedere, in relazione alle conoscenze acquisite in base al processo tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, ad adottare e ad aggiornare le idonee e preventive misure di sicurezza per i dati informatici in relazione ai trattamenti di diretta competenza ed a collaborare con i Responsabili Interni dell'Ente per la definizione delle

misure di sicurezza inerenti i trattamenti di competenza degli stessi;
b) programmare e realizzare gli interventi in materia di sicurezza informatica;
c) collaborare con il Titolare e i Responsabili interni per la definizione delle istruzioni operative per la sicurezza delle banche dati;
d) curare il coordinamento delle operazioni relative alla sicurezza delle categorie particolari di dati personali di cui agli artt. 9 e 10 del GDPR oggetto di trattamento con modalità informatica, provvedendo a prevenire i rischi di distruzione o perdita, anche accidentale;
e) fornire supporto ai Responsabili interni, sui profili informatici, per lo svolgimento della Valutazione di impatto di cui all'art. 35 del GDPR;
f) collaborare con le strutture interne alla tenuta dell'elenco degli amministratori di sistema ed assisterle nella nomina, nella formulazione delle istruzioni e nell'attività di verifica sull'operato degli amministratori stessi;

Art. 8 - Responsabile esterno del trattamento

1. I Dirigenti nominano quali responsabili del trattamento i soggetti pubblici o privati affidatari, per conto del Comune di Rosignano Marittimo, di attività e servizi che per la loro realizzazione rendono necessario il trattamento di dati personali o i soggetti terzi che trattano dati sulla base di specifiche convenzioni.

2. I Dirigenti provvedono a dare adeguate istruzioni per i trattamenti nel contratto di affidamento o con separato atto giuridico che definisca la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati oltre agli obblighi che il Responsabile esterno si impegna a rispettare con la sottoscrizione.

3. La nomina del Responsabile esterno del trattamento è fatta al momento dell'inizio dell'esecuzione se anteriore alla stipula del contratto.

4. I Responsabili esterni del trattamento sono nominati tra soggetti che forniscono le garanzie di cui all'art. 28 par. 1 GDPR. La sussistenza di tali garanzie deve essere espressamente dichiarata.

5. E' consentita, previa autorizzazione del Dirigente di cui al comma 1, la nomina di sub-responsabili da parte di ciascun Responsabile esterno per l'esecuzione di specifiche attività di trattamento ai sensi dell'art. 28 par. 4 GDPR.

ART. 9 - Incaricati al trattamento

1. I Responsabili interni del trattamento procedono a designare, all'interno della propria struttura operativa, il personale dipendente incaricato per l'espletamento di tutte le operazioni di trattamento dei dati.

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

3. Gli incaricati effettuano tutte le operazioni di trattamento dei dati nel rispetto delle istruzioni e direttive impartite dal Responsabile interno 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 di Rosignano Marittimo;
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.

Art. 10 - Amministratori di sistema

1. Il Dirigente responsabile della U.O. Sistemi informativi e Innovazione tecnologica, provvede a designare gli amministratori di sistema tra i propri dipendenti o, se necessario, tra soggetti esterni, nei casi e con le modalità stabilite dal Provvedimento del 27.11.2008 (e successive modifiche e integrazioni) del Garante della Privacy.

2. Qualora la designazione degli amministratori di sistema riguardi soggetti esterni all'Ente, la competenza è del Dirigente che ha provveduto all'affidamento del contratto in base al quale viene sviluppato o gestito il software, viene strutturata o gestita la banca dati informatica o, comunque, viene effettuato il trattamento.

Art. 11 - Responsabile della protezione dei dati (DPO)

1. Il Responsabile della protezione dei dati (in seguito indicato con "DPO") può essere individuato tra i dipendenti di ruolo dell'Ente, ovvero (in alternativa) all'esterno tra professionisti scelti secondo le modalità previste dal codice.

2. Il DPO può essere scelto fra i dipendenti dell'Ente di qualifica non inferiore alla cat. D, purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il Titolare ed il Responsabile del trattamento provvedono affinché il DPO mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

3. Nel caso in cui il DPO non sia un dipendente dell'Ente, l'incaricato è selezionato fra soggetti aventi le medesime qualità professionali richieste al dipendente, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili; i compiti attribuiti al DPO sono indicati in apposito contratto di servizio o incarico professionale. Il DPO esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di tale adempimento al Titolare del trattamento.

4. E' inoltre possibile l'affidamento dell'incarico di DPO ad un unico soggetto, anche esterno, designato da più Comuni mediante esercizio associato della funzione nelle forme previste dal D.Lgs. 18 agosto 2000 n. 267.

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

6. Il DPO, ferma restando l'indipendenza nello svolgimento dei compiti suoi propri, riferisce direttamente al Titolare e ai Responsabili interni del trattamento, e viene costantemente informato e coinvolto in tutte le decisioni riguardanti il trattamento dei dati personali.

7. Il DPO propone, in accordo con l'U.O. Segretariato 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.

8. Gli uffici formulano le proprie richieste al DPO dandone contestualmente conoscenza all'U. O. Segretariato. Il DPO rende noti i risultati della propria attività consultiva, di norma resa entro 30 giorni, anche all'U. O. Segretariato. Qualora la questione coinvolga più Unità Organizzative, l'Unità Organizzativa Segretariato ne dà adeguata diffusione per garantirne l'uniformità di applicazione.

9. Il DPO può convocare incontri con i responsabili interni e i dipendenti incaricati del trattamento per l'esecuzione dei propri compiti di informazione, consulenza, sorveglianza e consultazione e può altresì organizzare specifiche giornate di formazione.

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

Art. 12 – Attività di monitoraggio

1. Il Titolare del trattamento verifica periodicamente il corretto utilizzo degli strumenti e il rispetto di quanto previsto dalla normativa, dai regolamenti del Comune di Rosignano Marittimo e dei provvedimenti del Garante della protezione dei dati personali.

2. Durante le attività di monitoraggio, di norma, sono oggetto di verifica:
- la puntualità degli adempimenti effettuati tramite strutture interne o esterne;
- la gestione delle informative e dei consensi;
- gli adempimenti contrattuali dei Responsabili esterni del Trattamento;
- la tenuta dei Registri e la loro coerenza;
- la nomina degli amministratori di sistema e il loro operato;
- la gestione del sistema di video-sorveglianza;
- la tenuta degli strumenti di firma digitale;
- il rispetto dei tempi di conservazione;
- le modalità di esercizio dei diritti;

3. L'U.O. Sistemi informativi e Innovazione tecnologica svolge, anche su richiesta dei Responsabili interni, sessioni di audit interno o esterno, in modo casuale e/o a campione, sui trattamenti informatici svolti, sul corretto uso dei dispositivi di lavoro, sui sistemi informatici di competenza e sulle misure di sicurezza poste in essere per verificare l' affidabilità e sicurezza delle stesse.

TITOLO III

TRATTAMENTO DEI DATI PERSONALI

Art. 13 - Registro delle attività di trattamento

1. Il Comune di Rosignano Marittimo tiene un registro unico dei trattamenti contenente le informazioni di cui all' art. 30 del GDPR che elenca i trattamenti delle strutture dell'Ente secondo lo schema allegato al presente regolamento.

2. In occasione dell'aggiornamento dell'elenco dei procedimenti e comunque entro il 30 giugno di ciascun anno, le strutture/servizi provvedono a trasmettere alla U.O. Segretariato l'aggiornamento delle attività di trattamento con riferimento agli ambiti di competenza.

ART. 14 - Consenso dell'interessato

1. Il Comune di Rosignano Marittimo, in quanto soggetto pubblico, non deve chiedere il consenso dell'interessato al trattamento dei dati personali, purché il trattamento medesimo sia conforme ai fini istituzionali dell'Ente di cui all'art. 3 del presente regolamento.

2. Nei limitati casi in cui il consenso vada richiesto questo deve essere libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto.

ART. 15 - Informativa

1. L'interessato deve essere preventivamente informato, oralmente o per iscritto, secondo quanto previsto dagli artt. 13 e 14 GDPR.

2. L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice.

3. Nell'informativa devono essere comunicati anche i dati di contatto del Responsabile Interno che effettua il trattamento.

4. Ciascun Responsabile interno è tenuto ad aggiornare periodicamente le informative utilizzate.

5. E' ammesso l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica solo se in combinazione con l'informativa completa.

6. L'informativa deve essere resa disponibile negli uffici anche mediante affissione e/o pubblicata sul Sito web dell'Ente.

ART. 16 - Diritti dell'interessato

1. Per l'esercizio dei diritti di cui agli articoli da 15 a 22 del GDPR l'interessato presenta richiesta al Titolare del trattamento.

2. L'istanza può essere riferita a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali, comunque trattati, ed è presentata al Comune di Rosignano Marittimo, senza formalità (es. posta elettronica, lettera raccomandata, etc.), fatte salve le limitazioni di cui all'art. 23 GDPR, e agli artt. 2-undecies e 2-duodecis del D.LGS 196/2003 e le altre limitazioni previste dalla legge.

3. L'U.O. Segretariato provvede senza ritardo sulla richiesta, e comunque entro trenta giorni dal suo ricevimento. Se le operazioni necessarie per il riscontro alla richiesta sono complesse o ricorre altro giustificato motivo, il termine per il riscontro è di sessanta giorni.

4. Se il trattamento è effettuato da soggetti terzi per conto del Comune di Rosignano Marittimo, la richiesta viene presentata al Responsabile interno che ha provveduto alla nomina del Responsabile esterno del trattamento.

5. L'esercizio dei diritti dell'interessato è gratuito. Il rilascio di copie non è soggetto a rimborsi di diritti di riproduzione e di ricerca.

6. Se l'interessato ritiene che il trattamento dei dati personali non sia conforme alle disposizioni vigenti ovvero se la risposta ad un'istanza con cui esercita uno o più dei diritti non perviene nei tempi indicati o non è soddisfacente, può rivolgersi all'Autorità Giudiziaria o al Garante per la protezione dei dati personali, in quest'ultimo caso mediante un reclamo ai sensi dell'art. 77 del GDPR.

7. Si procede alla cancellazione dei dati personali in conformità alle norme sulla conservazione della documentazione amministrativa, una volta venute meno le finalità per le quali sono raccolti, fatti salvi gli adempimenti legati ad obblighi di legge o a finalità legali/difensive.

Art. 17 - Sicurezza del trattamento

1. Ciascun Responsabile interno mette in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio e procede, secondo una pianificazione concordata con il DPO, ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati.

2. Il Comune di Rosignano Marittimo individua all'interno dei codici di condotta specifiche previsioni per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto.

Art. 18 - Durata del trattamento

1. Fatto salvo quanto specificamente disposto da disposizioni di settore, la durata del trattamento dei dati personali coincide, di norma, con i tempi di conservazione indicati, in riferimento alle diverse tipologie documentali, nel Piano di conservazione dell'Ente e nel relativo Massimario di scarto. La durata dei trattamenti è indicata nel Registro Unico di cui all'art. 13.

ART. 19 - Valutazione di impatto

1. Ciascun Responsabile interno valuta la necessità di sottoporre a valutazione di impatto i trattamenti da effettuare e/o le proprie banche dati; qualora decida di procedere a valutazione di impatto si coordina con il DPO e, in caso di trattamento con modalità informatica, con la U.O. Sistemi informativi e Innovazione tecnologica per programmarne le modalità operative.

2. La valutazione di impatto dovrà essere prioritariamente effettuata sulle banche dati condivise.

Art. 20 - Violazione dei dati personali

1. Chiunque venga a conoscenza di una violazione dei dati personali (data breach) è tenuto a segnalarlo, anche per il tramite del proprio responsabile, al Responsabile interno competente che deve provvedere tempestivamente a comunicarlo al titolare del trattamento

2. Il Titolare ove possibile, notifica la violazione dei dati personali al Garante della protezione dei dati personali entro 72 ore dal momento in cui ne sia venuto a conoscenza, a meno che sia improbabile che la stessa violazione presenti un rischio per la tutela dei diritti e delle libertà delle persone fisiche.

3. La notifica viene effettuata, prevedendo almeno gli elementi indicati al paragrafo 3 dell'articolo 33 del GDPR. La notifica al Garante della protezione dei dati personali effettuata oltre le 72 ore, deve essere motivata.

4. Le segnalazioni e le notifiche dei casi di violazione dei dati personali sono comunicati tempestivamente dai Responsabili interni alla Unità Organizzativa Sistemi Informativi e Innovazione tecnologica e alla Unità Organizzativa Segretariato che informa il DPO.

5. Ciascun Responsabile interno 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 per poter dimostrare il rispetto delle disposizioni del GDPR.

7. Il Responsabile interno provvede ad annotare le violazioni di dati personali che si sono verificate all'interno del proprio Settore o che siano state comunicate dai Responsabili esterni, ai quali ha affidato servizi che implicano il trattamento di dati personali nel Registro dei data breach.

8. Il Registro dei data breach è tenuto presso la U.O. Segretariato. In esso vengono registrate le seguenti violazioni:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali

Il registro contiene le seguenti informazioni:

- dettagli relativi al Data Breach (e cioè la causa, il luogo dove è avvenuto e la tipologia di Dati personali violati);
- gli effetti e le conseguenze della violazione e il piano di intervento predisposto dal Titolare.

Art. 21 - Formazione del personale

1. Il Comune di Rosignano Marittimo assicura la programmazione e l'organizzazione delle attività formative del personale per la corretta applicazione delle disposizioni in materia di trattamento dei dati personali anche sulla base delle indicazioni del DPO.

Art. 22 - Trattamento dei dati personali da parte di Amministratori

1. Gli Amministratori, come definiti dall'art. 77 c. 2 del D.Lgs. 267/2000, sono legittimati al trattamento dei dati personali esclusivamente nell'esercizio delle proprie funzioni istituzionali e sono tenuti alla riservatezza; in tale esercizio devono assicurare il rispetto del GDPR.

ART. 23 - Comunicazione e diffusione dei dati personali comuni

1. La comunicazione dei dati personali all'interno dell'Ente per lo svolgimento delle funzioni istituzionali non è soggetta a limitazioni, salvo quelle espressamente previste da leggi e regolamenti.

2. Ciascun Responsabile interno, valutato il caso, può decidere di adottare le misure necessarie alla tutela della riservatezza degli interessati.

3. La comunicazione dei dati personali ad altri soggetti pubblici e la loro diffusione è disciplinata dall'art. 2 ter del D.Lgs. 196/2003.

ART. 24 - Norma finale

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni di cui al GDPR, al D.Lgs. 196/03 (Codice Privacy) e ss.mm.ii. e ai Regolamenti comunali vigenti.