# COMUNE DI DECIMOMANNU

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

Approvato con deliberazione del Consiglio comunale n. 44 del 14.11.2024

## 1. INTRODUZIONE

Il 24.05.2016 è entrato in vigore il Regolamento UE n. 2016/679 (in seguito, "Regolamento"; "GDPR") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. L'impronta del Regolamento impone un maggior rigore nella gestione dei trattamenti e degli adempimenti più articolati e incisivi a fronte di una necessaria maggiore cautela nel trattamento dei dati. In particolare, il nuovo Regolamento europeo ha come oggetto la tutela delle persone con riguardo al trattamento e alla circolazione dei dati; il principio cardine è, infatti, la tutela del diritto e della libertà fondamentale alla protezione dei dati nonché i principi generali della portabilità e circolazione dei dati personali nell'UE (artt. 1, 2, 3 GDPR).
In questo contesto il regolamento comunale in materia di *privacy* rappresenta uno strumento utile per ottenere un maggiore equilibrio tra i contrapposti interessi dei soggetti coinvolti come, ad esempio, il rapporto tra l'Ente, i cittadini, i funzionari e dipendenti comunali, le imprese e tutte le organizzazioni del territorio.

Il Comune è da tempo impegnato nel perseguire politiche di rispetto della tutela dei dati personali, avendo già fatto propri i principi cardine in tema di *privacy*, quale elemento di protezione e valorizzazione della propria attività pubblicistica.

Al fine di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, Il Comune di Decimomannu a partire dall'anno 2018, ha avviato un processo di aggiornamento e revisione delle attività connesse alla protezione dei dati personali, al fine di consentire un innalzamento dell'attuale livello di protezione di questi ultimi.

A tal fine, l'Ente si è dotato di un sistema di regole e procedure al fine di poter essere costantemente aggiornato in materia, in linea con l'esperienza maturata dall'Ente e con le evoluzioni normative. Il Comune adotta il presente regolamento, al fine di dotarsi di strumenti di "*governance*" e di presidi organizzativi in linea con le nuove previsioni del Regolamento europeo.

### 1.1 Premessa

Il presente documento è redatto seguendo quanto previsto dal GDPR e dalla normativa italiana, oltreché dai Provvedimenti dell'Autorità Garante per la protezione dei dati personali (di seguito Autorità Garante o Autorità di controllo) che risultino essere applicabili alle attività esplicate dal Comune di Decimomannu ("Normativa *Privacy*").
Il presente documento verrà aggiornato ed approvato in caso di modificazioni della normativa che implichino una modifica degli assetti e delle procedure adottate dal Comune ovvero allorquando vengano adottate decisioni che comportino la migliore adesione ai principi del Regolamento europeo 2016/679 ovvero la migliore rispondenza alle esigenze dei soggetti facenti parte del sistema privacy, primi fra tutti gli interessati.

### 1.2 Termini e definizioni

Si riportano alcune definizione chiave in ambito privacy:
**Amministratore di sistema:** Il soggetto preposto alla gestione di sistemi informatici con i quali vengono effettuati Trattamenti di Dati Personali.
**Autenticazione informatica**: L'insieme degli strumenti elettronici e delle procedure attraverso il quale viene verificata la corretta Identità di un utente.
**Autorità di controllo:** Si intende l'Autorità di cui all'articolo 51 del Regolamento Europeo in Materia di Protezione dei Dati Personali – *General Data Protection Regulation* [GDPR, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016], ovvero una o più Autorità pubbliche indipendenti incaricate da uno Stato Membro di vigilare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali.

**Banca dati:** Una banca dati è una raccolta di informazioni/dati, in forma cartacea o informatica, organizzati in modo strutturato e omogeneo, in modo da poter essere facilmente reperite, aggiornate e modificate attraverso l'utilizzo di apposite chiavi di ricerca.
**Cancellazione sicura:** Eliminazione di dati presenti sul supporto elettronico con modalità che li rendano inintelligibili e non recuperabili.
**Comunicazione:** la trasmissione di dati personali a soggetti determinati
**Credenziali di autenticazione:** I dati e i dispositivi, assegnati a un soggetto e a esso univocamente correlati, utilizzati per l'autenticazione informatica.
**Danno:** Conseguenza pregiudizievole derivante dal concretizzarsi di una minaccia.
***Data Breach*:** Violazione della sicurezza che comporta, accidentalmente o volontariamente, la distruzione, perdita, alterazione, pubblicazione o accesso non autorizzato di dati personali trasmessi, conservati o in altro modo trattati.
***Data Protection Officer* o DPO:** Soggetto designato dal Titolare del trattamento in funzione delle sue qualità professionali al fine di informare e fornire consulenza al Titolare stesso nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla Normativa *Privacy*.
**Dato anonimo:** Il dato che in origine, o a seguito di trattamento, non si riferisce a una persona fisica identificata o identificabile.
**Dati appartenenti a particolari categorie:** I dati personali indicati all'art.9 del GDPR idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
**Dati giudiziari:** I dati personali relativi a condanne penali e reati di cui al'art. 10 del GDPR, nonché i dati idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da *a)* a *o)* e da *r)* a *u)*, del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
**Dato personale:** Qualsiasi informazione riguardante una persona fisica identificata o identificabile. 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.
**Diffusione:** La trasmissione di dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
**Informazione:** Trasmissione dei dati e l'insieme delle strutture che la consentono.
**Interessato:** La persona fisica identificata o identificabile mediante i dati personali trattati.
**Minaccia:** evento il cui concretizzarsi potrebbe arrecare un danno ai beni dell'Ente.
**Misure adeguate:** L'insieme delle misure tecniche e organizzative volte a garantire la liceità del trattamento effettuato, anche con riferimento alla disponibilità, autenticità, integrità e la riservatezza dei dati personali conservati o trasmessi, individuate sulla base e in relazione ai rischi individuati rispetto ad una determinata attività di trattamento.
**Normativa Privacy:** Complessivamente, il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, la normativa italiana di riferimento (in particolare, il D.Lgs. 196/2003, come modificato e integrato dal D.Lgs. 101/2018 di adeguamento, nonché le regole di condotta/regole tecniche ad esso allegate e i Provvedimenti dell'Autorità Garante per la protezione dei dati personali applicabili al contesto) nonché i provvedimenti dell'European Data Protection Board (EDPB). .
**Persone Designate/Autorizzate al trattamento:** Le persone fisiche autorizzate dal Comune a compiere operazioni di trattamento dei dati personali, nell'ambito e sotto l'autorità del Comune stesso, in ottemperanza alle istruzioni ricevute mediante apposita nomina.
**Responsabile del trattamento:** La persona giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento, appositamente nominata ai sensi e in conformità all'art. 28 del GDPR.

**Rischio:** Possibilità che un evento non voluto e potenzialmente dannoso si verifichi, facendo venir meno la riservatezza e/o integrità e/o disponibilità dei dati personali e, quindi, mettendo a repentaglio la tutela dei diritti e le libertà delle persone fisiche.
**Sistema di autorizzazione:** L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
**Titolare del trattamento o Titolare:** 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.
**Trattamento:** Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la 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.

### 1.3 Obiettivi

Il presente Regolamento definisce la portata e l' attuazione della Normativa *Privacy* all'interno del Comune. In particolare, delinea un sistema organico e strutturato di gestione di tutti gli aspetti concernenti i profili "*privacy*" attraverso un modello di gestione uniforme, fornendo ai soggetti che di tale sistema fanno parte indicazioni chiare, sia sul piano tecnico/operativo che sul piano organizzativo, sulle modalità di applicazione della Normativa *Privacy*.
Il presente documento, pertanto:

- Definisce i requisiti per il trattamento dei dati personali, affinché esso avvenga, all'interno del quadro delineato dalla Normativa *Privacy*, nel rispetto delle prescrizioni previste dalla normativa stessa e individua – disciplinandone le modalità – gli adempimenti da porre in essere per garantire la conformità alla normativa in parola;
- Fornisce indicazioni sulle modalità di trattamento dei dati personali;
- Individua le misure tecniche ed organizzative che il Comune adotta per garantire – ed essere in grado di dimostrare – la conformità alla Normativa Privacy delle attività di trattamento dei dati delle persone fisiche che il Comune effettua direttamente, oppure avvalendosi di soggetti terzi;
- Disciplina i ruoli e le responsabilità in modo da evitare la possibile irrogazione delle sanzioni amministrative pecuniarie;

Obiettivo ulteriore del presente documento è quello, di concerto con le attività formative che verranno poste in essere, di innalzare la cultura di una corretta e sicura gesti ne dei dati personali e consentire il rispetto e l'effettiva operatività del Sistema di gestione *privacy* qui delineato.

## 2. MODELLO ORGANIZZATIVO: RUOLI E RESPONSABILITÀ

Di seguito vengono presentati i ruoli chiave identificati del regolamento:

1. Interessato;
2. Titolare del Trattamento;
3. Responsabile del Trattamento;
4. Designati/Autorizzati al Trattamento;
5. Persona Autorizzata al trattamento di Videosorveglianza;
6. DPO;
7. Amministratore di Sistema;
8. Referente privacy/Privacy officer;

Per ciascuna delle seguenti figure, di seguito sono descritti elementi tipici ed eventuali responsabilità e ruoli definiti nell'ambito del Regolamento.

### 2.1 Interessato

Con il termine "Interessato" si fa riferimento alla persona fisica resa identificata o identificabile dai dati personali trattati.

**2.2 Titolare del trattamento**

Il "Titolare" è la persona fisica/giuridica che determina le finalità e i mezzi del trattamento dei dati personali, oppure che viene individuato come tale dalla legge stessa che prevede e disciplina le attività che comportano il trattamento di dati personali.

Il Titolare ha la facoltà di nominare "Persone Designate/Autorizzate al Trattamento",attribuendo ad esse specifici compiti e funzioni connessi al trattamento dei dati personali operanti sotto la propria autorità.

**2.3 Responsabile esterno al Trattamento**

Ai sensi dell'art. 28 del GDPR, il "Designato/Responsabile del Trattamento" è la persona fisica/giuridicache tratta dati personali per conto del Titolare e da quest'ultimo espressamente nominato e da cui riceverà istruzioni circa le modalità di trattamento dei dati ad esso affidati. Quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. Il trattamento dei dati da parte di un Responsabile è disciplinato da un contratto o altro atto giuridicamente vincolante che connetta direttamente il Responsabile alle indicazioni fornite dal Titolare del trattamento relativamente a:

- oggetto e la durata del trattamento dei dati;
- natura e le finalità del trattamento;
- tipo di dati personali e le categorie di soggetti interessati;
- istruzioni/restrizioni per qualsiasi trasferimento di dati personali sia all'interno che all'esterno del Comune;
- applicazione di misure di sicurezza adeguate;
- diritti del Titolare del trattamento;
- obblighi del Responsabile del trattamento.

Si indicano, qui di seguito, i principali obblighi del Responsabile:

1. assicurarsi che il trattamento dei Dati Personali avvenga secondo le istruzioni impartite dal Titolare;
2. assicurarsi che sia garantito l'esercizio dei diritti da parte degli interessati;
3. procedere all'identificazione delle Persone Autorizzate al trattamento, fornendo alle stesse adeguate istruzioni in relazione al Trattamento effettuato/da effettuare;
4. garantire che le Persone Autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
5. adottare tutte le misure richieste ai sensi dell'articolo 32 del GDPR;
6. assistere il Titolare del trattamento nel garantire il rispetto degli obblighi del GDPR;
7. garantire l'applicazione di misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
8. mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi normativi applicabili e a consentire/contribuire alle attività di revisione, comprese le verifiche;
9. garantire l'adozione di adeguate misure tecniche e organizzative che garantiscano un adeguato livello di protezione dei Dati Personali trattati, nel rispetto delle leggi applicabili;
10. garantire che l'eventuale dismissione di strumenti elettronici contenenti Dati Personali avvenga nel rispetto delle leggi applicabili;
11. cooperare con il Titolare del trattamento nella rilevazione e gestione di potenziali violazioni dei Dati Personali (*Data Breach*), garantendo la necessaria collaborazione nelle attività di *recovery* che dovessero rendersi necessarie;
12. non ricorrere a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento;
13. su scelta del Titolare del trattamento, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che legge preveda la conservazione dei dati.

**2.4 Designati ed Autorizzati al Trattamento**

Le “Persone Designati ed Autorizzati al trattamento” sono soggetti interni all’organizzazione del Comune all’uopo designati/autorizzati dal Titolare, nell’ambito dei rispettivi ruoli e funzioni.

Ciascun dipendente dell’Ente potrà svolgere la funzioni di:

- Designato (coloro cui sono attribuiti compiti di coordinamento e supervisione in funzione delle competenze svolte, nel rispetto dell’organigramma comunale )
- Autorizzato (ovvero tutti i dipendenti e collaboratori)

Operano secondo le istruzioni fornite dal Titolare. Le suddette istruzioni possono essere differenziate e aggiornate nel corso della durata del rapporto in ragione di specifiche necessità (cambio mansione/responsabilità/attività).

Principali compiti assegnati ai Designati al trattamento:

- assicurarsi che il trattamento dei Dati Personali avvenga secondo le istruzioni impartite dal Titolare;
- assicurarsi che sia garantito l’esercizio dei diritti da parte degli interessati;
- procedere all’identificazione delle Persone Autorizzate al trattamento, fornendo alle stesse adeguate istruzioni in relazione al Trattamento effettuato/da effettuare;
- garantire che le Persone Autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure richieste ai sensi dell’articolo 32 del GDPR;
- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi del GDPR;
- garantire l’applicazione di misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi normativi applicabili e a consentire/contribuire alle attività di revisione, comprese le verifiche;
- garantire l’adozione di adeguate misure tecniche e organizzative che garantiscano un adeguato livello di protezione dei Dati Personali trattati, nel rispetto delle leggi applicabili;
- garantire che l’eventuale dismissione di strumenti elettronici contenenti Dati Personali avvenga nel rispetto delle leggi applicabili;
- cooperare ed assistere il Titolare nella compilazione del Registro dei Trattamenti;
- cooperare con il Titolare del trattamento nella rilevazione e gestione di potenziali violazioni dei dati personali (*Data Breach*), garantendo la necessaria collaborazione nelle attività di *recovery* che dovessero rendersi necessarie;

Principali obblighi in capo alle persone Autorizzate al Trattamento:

- eseguire le proprie attività lavorative nel rispetto delle normative applicabili e delle istruzioni ricevute dal Titolare e Designati in merito alle corrette modalità di gestione dei dati personali;
- trattare e custodire i dati personali, in particolare quelli sensibili, a cui si ha accesso nell’espletamento delle mansioni lavorative, garantendo l'adozione/applicazione delle misure di sicurezza disposte dal Titolare/Responsabile del Trattamento di riferimento, al fine di evitarne la distruzione, la perdita o l’accesso da parte di persone non autorizzate;
- trattare i dati esclusivamente al fine di adempiere alle obbligazioni conferite e, in ogni caso, per scopi determinati, espliciti e, comunque, in termini compatibili con gli scopi di riservatezza per i quali i dati sono stati raccolti;
- verificare costantemente la correttezza dei dati trattati e, ove necessario, provvedere al loro aggiornamento;
- garantire, in ogni operazione di trattamento, la massima riservatezza, astenendosi dal trasferire, comunicare e/o diffondere i dati a terzi, salvo preventiva autorizzazione del Titolare o del Responsabile del Trattamento di riferimento;
- partecipare alle iniziative formative su tematiche *Privacy*;

- segnalare al Titolare o al Designato di riferimento eventuali criticità o punti di attenzione inerenti alla gestione della *Privacy* (per esempio: possibile *Data Breach*, nuovi progetti o servizi con impatti Privacy, problematiche nella gestione dei diritti degli interessati, nuove terze parti cui vengono trasferiti dati personali);
- adottare le misure per evitare l'accesso dei dati a terze parti durante l'allontanamento, anche temporaneo, dalla postazione di lavoro.

**2.5 DPO**

Il Responsabile Protezione dei Dati – DPO è nominato dal Titolare del Trattamento, potrà essere interno od esterno al Comune, svolge, ex art. 39 GDPR le seguenti funzioni:

a) fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. Svolgere le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare, dei designati ed autorizzati e dei Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare e mappare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) ogni altra competenza prevista dall' art 39 GDPR

**2.6 Persona Autorizzata al trattamento della Videosorveglianza**

La "Persona Autorizzata al trattamento della Videosorveglianza" è la persona fisica, autorizzata dal Titolare, a compiere operazioni di Trattamento sulle immagini, registrate e non, dai sistemi di videosorveglianza presenti all'interno del territorio comunale. La sua figura viene meglio dettagliata nell'apposito Regolamento sulla Videosorveglianza del Comune.

**2.7 Amministratore di Sistema**

L' "Amministratore di Sistema" è il soggetto preposto alla gestione di sistemi informatici con i quali vengono effettuati Trattamenti di Dati Personali.

Di seguito elencati i principali obblighi:

- monitorare lo stato dei sistemi di elaborazione e delle banche dati del Comune, con particolare e costante attenzione al profilo della sicurezza;
- verificare che l'accesso ai sistemi e ai dati personali ivi contenuti sia debitamente protetto, nonché consentito solo quando strettamente necessario, nel pieno rispetto della legge e delle *policy* aziendali;
- supportare la struttura di ICT nella definizione ed implementazione di misure tecniche ed organizzative tali da garantire un livello di sicurezza adeguato al rischio, tra cui, a titolo esemplificativo e non esaustivo: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità del Comune di assicurare, su base permanente, riservatezza, integrità, disponibilità e resilienza dei sistemi, oltre a quella di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico (*Data*

*Breach*); c) l'esecuzione di controlli ed *audit* per testare, verificare e valutare regolarmente l'efficacia delle misure adottate per garantire la sicurezza dei trattamenti;
- adempiere a tutti gli obblighi stabiliti dalla normativa vigente e dalle specifiche *policy* adottate dal Comune;
- effettuare gli interventi di manutenzione necessari;
- verificare, con continuità, il corretto funzionamento dei sistemi di *backup*/*recovery*;
- sovrintendere all'operato di eventuali tecnici esterni che, a qualunque titolo, si trovino ad operare su sistemi o archivi di dati rientranti nel proprio perimetro di competenza;
- gestire i sistemi di autenticazione e autorizzazione comunali, nonché l'assegnazione delle relative credenziali a tutti i dipendenti del Comune;
- avvisare senza ingiustificato ritardo il Comune riguardo a qualsiasi violazione della sicurezza da cui possa derivare, in maniera accidentale o illecita, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati o conservati nei sistemi del Comune;
- prestare la massima collaborazione nei confronti di ogni Responsabile del Trattamento eventualmente nominato dal Comune.

**2.8 Referente Privacy Privacy Officer**

È il soggetto identificato dal Titolare che, per specificità delle proprie funzioni, ha compiti di attuare il modello organizzativo privacy dell'Ente nonché di formare i documenti e gli atti necessari all'Amministrazione per l'attuazione dei principi del GDPR e delle ulteriori fonti normative. E' il riferimento interno all'organizzazione per il personale di quest'ultima ed ha la funzione di raccordo tra il Titolare, il DPO e l'amministratore di sistema. Viene individuato all'interno secondo le scelte organizzative dell'Amministrazione dal Titolare

**2.9 Organizzazione interna del Comune in materia di privacy**

Il Titolare del trattamento dei dati, si avvale delle competenze e funzioni dei soggetti individuati nei precedenti punti così da consentire una maggiore tempestività di intervento e celerità decisionale, nell'ambito dell'ordinaria gestione del Comune. In particolare il Titolare predisporrà un modello organizzativo privacy per l'Amministrazione al fine di:
- assicurare che l'organizzazione, le misure di sicurezza e procedurali adottate e le modalità operativo/gestionali del Comune siano conformi ai requisiti definiti dalla normativa *Privacy*;
- assicurare costantemente che i compiti e le responsabilità in materia di protezione dei dati personali siano allocati in modo chiaro e appropriato, in modo coerente con le mansioni lavorative e le funzioni assegnate;
- in generale, assicurare che il Comune adempia agli obblighi che la normativa pone in capo al Titolare ed ai designati, autorizzati e al Responsabile del trattamento, assumendo le iniziative necessarie e curando l'adozione degli atti formali (incluse la predisposizione e l'approvazione, la modifica e la conservazione della documentazione prevista dalla normativa in parola e dalle presenti Linee Guida, nonché delle Linee Guida stesse).

È compito del Titolare sovraintendere alla gestione dei processi e curare gli adempimenti previsti dalla normativa. Pertanto, gli sono affidati i seguenti compiti:
- organizzare, gestire e supervisionare tutte le operazioni di trattamento di dati personali effettuate dai dipendenti e collaboratori del Comune di concerto con il DPO ed i Dirigenti, in modo che il trattamento dei dati personali avvenga nel rispetto dei principi previsti dall'art. 5 del Regolamento europeo (liceità, correttezza e trasparenza, esattezza, integrità e riservatezza, limitazione delle finalità e della conservazione, minimizzazione dei dati trattati in relazione alle attività svolte);
- nominare i designati ed autorizzati, gli eventuali amministratori di sistema o responsabili, o comunque fornire delega ai designati per procedere alla nomina;
- valutare, di concerto con il DPO, i rischi correlati alle attività di trattamento dei dati personali, tenuto conto delle modalità operative del Comune, dell'organizzazione e delle misure di sicurezza implementate e, al ricorrere dei relativi presupposti, effettuare la valutazione di impatto (DPIA);

- assicurare la presenza delle misure tecniche e organizzative individuate ai sensi dell'art. 32 del Regolamento europeo, monitorandone costantemente l'adeguatezza e la corretta applicazione e di concerto con il deputato reparto tecnico/informatico e il DPO;
- gestire le attività necessarie per consentire l'esercizio dei diritti da parte degli interessati, al fine di fornire riscontro alle loro istanze, provvedendo anche all'alimentazione e conservazione dell'apposito Registro di con concerto con i dirigenti, le posizioni operative ed il DPO;
- gestire il processo di *data breach*, provvedendo anche all'alimentazione e conservazione dell'apposito Registro e all'eventuale notifica della violazione al Garante per la protezione dei dati personali, di concerto con i designati, le posizioni operative ed il DPO;

Il Titolare individua i Designati, negli ambiti di rispettiva competenza e sulla base dei ruoli e responsabilità assegnati nonchè in funzione delle mansioni svolte, nel rispetto dell'Organigramma Comunale a cui sono attribuiti compiti di coordinamento e supervisione. I designati sopra indicati, ricoprono ruoli di responsabilità perle quali il Titolare predispone apposita lettera/nomina di incarico ed autorizzazione al trattamento.
I designati sono tenuti ad avere una particolare attenzione in merito all'applicazione delle norme in materia di *privacy* e del presente Regolamento e sorvegliarne l'applicazione da parte del personale che ad essi fa capo.

**I**l Titolare provvede ad autorizzare al trattamento dei dati personali, a mezzo apposito atto di nomina ed incarico, ciascun dipendente e collaboratore, anche a mezzo dei designati, al fine di garantire che, nell'ambito delle mansioni attribuite, siano adottate le misure di sicurezza a protezione dei dati personali nei termini riportati nel presente Regolamento.
I soggetti in parola sono autorizzati al trattamento dei dati per le sole finalità individuate ed è vietato qualsiasi altro uso dei dati personali trattati che non sia in linea con l'incarico ricevuto.
Le Persone Autorizzate al Trattamento verranno formalmente edotte in merito alla circostanza che:
a) il trattamento e la conservazione dei dati deve avvenire in modo lecito e proporzionato alle funzioni comunali, nel rispetto della riservatezza;
b) la raccolta, registrazione ed elaborazione dei dati, mediante strumento elettronico o cartaceo, deve essere limitata alle necessità comunali;
c) è onere dei soggetti autorizzati correggere o aggiornare i dati posseduti.

Al momento della formalizzazione della nomina, l'autorizzato riceve le idonee informazioni e istruzioni.

**3. <u>GESTIONE DEI DATI PERSONALI</u>**
Il Comune garantisce che i dati raccolti siano completi, accurati e mantenuti aggiornati rispetto alle finalità per cui vengono raccolti, compatibilmente con le tempistiche necessarie per gli eventuali aggiornamenti e tenuto conto del numero di dati oggetto di trattamento.
I dati personali sono raccolti dal Comune per finalità specifiche, esplicite e legittime, mai in eccesso e comunque in coerenza con le finalità previste.
Come previsto dal Regolamento, gli Interessati hanno la facoltà di esercitare i seguenti diritti in merito ai propri Dati Personali:
- **diritto di accesso** (art. 15): ovvero il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e, in tal caso, di ottenere l'accesso a tali dati personali, ottenendone copia, ed alle informazioni di cui all'art. 15 del Regolamento;
- **diritto di rettifica** (art. 16): ovvero il diritto di ottenere la rettifica dei dati inesatti che lo riguardano o l'integrazione dei dati incompleti;
- **diritto alla cancellazione** (art.17): ovvero il diritto di ottenere la cancellazione dei dati che lo riguardano, se sussiste uno dei motivi indicati dall'art. 17 del Regolamento;
- **diritto di limitazione di trattamento** (art. 18): ovvero il diritto di ottenere, nei casi previsti dal medesimo articolo, la cancellazione/pseudonimizzazione/anonimizzazione dei dati personali che lo riguardano con l'obiettivo di limitarne il trattamento;
- **diritto alla portabilità dei dati** (art. 20): ovvero il diritto, nei casi indicati da medesimo articolo, il trattamento effettuato con mezzi automatizzati, basato sul consenso o sull'esecuzione di un contratto), di

ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati che lo riguardano, nonché di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti;
- **diritto di opposizione** (art. 21): ovvero il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento – fondato sul perseguimento di un legittimo interesse da parte del Titolare – dei dati personali che lo riguardano, compresa la profilazione sulla base di tali disposizioni;
- **diritto ad ottenere un processo decisionale non completamente automatizzato** (art. 22): ovvero il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, salvo i casi previsti dall'art. 22 del Regolamento.
Per dare seguito alle richieste di esercizio dei diritti degli interessati, l'Amministrazione provvederà a dotarsi e rendere pubblica e conoscibile apposita procedura dotata di relativi atti a disposizione degli interessati nel sito web istituzionale nonché in formato cartaceo presso ogni ufficio comunale.

### 3.1 Fasi del ciclo di vita del dato personale

Le operazioni di trattamento dei dati personali devono essere strettamente limitate al perseguimento delle finalità indicate nelle relative informative, così come verranno pubblicate sul sito istituzionale. Di seguito sono riportate le fasi del "ciclo di vita" del dato personale, nonché il dettaglio delle modalità di gestione operativa

#### 3.1.1 Raccolta

Per quanto concerne la raccolta dei dati, l'acquisizione – direttamente presso gli interessati, oppure mediante trasmissione/comunicazione da soggetti terzi Titolari o Responsabili del trattamento – può avvenire mediante differenti canali, digitali (siti *web*, posta elettronica) e non digitali (Posta ordinaria, portineria, uffici, fax). Il Comune effettua operazioni di trattamento sulle categorie di Dati Personali indicate nel Registro delle Attività di trattamento predisposto ai sensi dell'art. 30, commi 1 e 2, del GDPR. Il Trattamento dei Dati Personali da parte del Comune deve avvenire per il perseguimento di finalità legittime individuate anticipatamente e comunicate agli interessati con le modalità e le tempistiche individuate dagli artt. 13 e 14 del GDPR. I principi di trattamento corretto e trasparente implicano che l'interessato sia debitamente informato, per iscritto oppure oralmente, in maniera concisa e utilizzando un linguaggio semplice e chiaro, in merito al trattamento di dati personali che lo riguardano.

#### 3.1.2 Cessazione del trattamento e Cancellazione

Nel caso in cui il Comune intenda cessare lo svolgimento di una o più operazioni di Trattamento, i sati personali precedentemente utilizzati nel contesto di tali operazioni dovranno essere distrutti, fatti salvi gli adempimenti legati ad obblighi di legge o a finalità legali/difensive. Il Comune provvede alla distruzione dei documenti e alla cancellazione dai supporti informatici che, dopo essere stati utilizzati per il Trattamento, siano destinati ad altro scopo, in accordo a quanto previsto dalla normativa. Tale cancellazione serve a prevenire la diffusione, anche accidentale, di dati personali con conseguente violazione (*Data Breach*) di cui agli articoli 33 e 34 del GDPR.
Nel caso in cui i Trattamenti cessati siano stati oggetto di precedente notifica all'Autorità Garante, il Comune dovrà prontamente provvedere ad effettuare i necessari aggiornamenti.

#### 3.1.3 Altre operazioni di Trattamento

Le operazioni di Trattamento effettuate dal Comune devono attenersi ai principi generali riportati di seguito:
- **Liceità, correttezza e trasparenza:** i dati devono essere trattati in modo conforme alle norme, nel rispetto reciproco delle parti ed in maniera trasparente nei confronti dell'Interessato;
- **Limitazione delle finalità:** i dati devono essere raccolti per finalità esclusivamente determinate, esplicite e legittime ed utilizzati in altre operazioni del trattamento solo laddove esse siano compatibili in quanto

connesse e consequenziali a quelle principali per il perseguimento delle quali si è proceduto alla raccolta dei dati;
- **Minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono raccolti;
- **Esattezza:** i dati devono essere esatti e, se necessario, aggiornati. Saranno adottate tutte le misure necessarie ed adeguate per garantire l'esattezza dei dati raccolti;
- **Limitazione della conservazione:** i dati devono essere conservati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario e alle finalità per le quali sono stati trattati. La durata della conservazione sarà indicata nell'informativa fornita all'interessato ovvero, laddove ciò non dovesse essere possibile in quanto non determinata dalla legge, saranno indicati i criteri in base ai quali viene individuato detto periodo;
- **Integrità e riservatezza**: i dati devono essere trattati in maniera da garantire la loro sicurezza e protezione. Il Comune di Decimomannu adotta tutte le misure idonee ed adeguate tenendo conto dello stato dell'arte e dei costi di attuazione, in grado di assicurare tali sicurezza e protezione. Il Comune di Decimomannu adotta, nel rispetto dei principi di *privacy by design* e *privacy by default* applicati nella progettazione dei sistemi e delle procedure, misure di sicurezza quali la pseudonimizzazione, la cifratura, l'oscuramento dei dati personali nonché le misure che garantiscono la continuità dei trattamenti e la disponibilità ed integrità dei dati quali, fra gli altri, costanti back up e misure di disaster recovery. Sempre nell'ambito dello stato dell'arte e dei costi di attuazione il Comune di Decimomannu procederà all'implementazione di tutte le misure che consentano la prevenzione e gestione delle violazioni dei dati personali.

### 3.2 Registro delle Attività di Trattamento

Il Comune di Decimomannu adegua il proprio registro delle attività di trattamento, **secondo lo schema di cui all'allegato1** costituente parte integrante e sostanziale del proprio modello organizzativo *privacy*.
Il registro delle attività di trattamento è lo strumento che raccoglie tutte le attività di trattamento dei dati personali svolte nel Comune, tenuto dal Titolare e/o dal Designato o da suo rappresentante come stabilito dall'art. 30 del GDPR. Il registro delle attività di trattamento è, quindi, fondamentale, non soltanto per disporre di un quadro aggiornato dei trattamenti in essere all'interno del Comune di Decimomannu, ma è anche indispensabile per ogni valutazione e successiva analisi del rischio. È quindi dovere dell'Amministrazione, di concerto con il DPO, mantenere costantemente aggiornamento il Registro con i nuovi trattamenti, nuove banche dati e nuove responsabilità, così come procedere all'eliminazione di eventuali trattamenti cessati. Sarà responsabilità di ciascun Designato provvedere a comunicare al DPO eventuali cambiamenti relativi ai Trattamenti in essere. Oltre al continuo aggiornamento, ogni sei mesi il Titolare ed i Designati insieme al DPO procederanno al riscontro e monitoraggio dell'esattezza e conformità del Registro.
Quale attività propedeutica all'elaborazione e redazione del Registro ex art.30 GDPR, si è proceduto all'individuazione e mappatura dei trattamenti eseguiti nei singoli Settori dell'Amministrazione.

## 4. PRIVACY BY DESIGN E BY DEFAULT

I suddetti principi sono menzionati nell'articolo 25 del Regolamento Generale Europeo per la Protezione dei Dati Personali ("*General Data Protection Regulation*" o GDPR) che impone al Titolare del trattamento l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti.
La *Privacy by Design* definisce una serie di principi che evidenziano l'importanza che la *privacy* dovrebbe rivestire in qualsiasi ambito, scelta o azione intrapresa da parte dei soggetti ed entità chiamati a conformarsi al nuovo GDPR.
La *Privacy by Design* si articola nei principi generali di seguito elencati:

1. Adozione di un approccio proattivo e non reattivo;
2. Definizione della *privacy* come parametro di default;
3. Necessità di tenere in considerazione i rischi *privacy* fin dalle fasi di progettazione di un nuovo trattamento e/o di un sistema che tratti dati personali;

4. Rispetto per tutte le esigenze;
5. Applicazione della sicurezza sull'intero ciclo di vita;
6. Visibilità e trasparenza;
7. Centralità dell'utente.

La *Privacy by Default* indica il principio secondo cui il trattamento dei dati personali richiesti ed utilizzati deve essere nella misura necessaria e sufficiente alle finalità previste e per il periodo strettamente necessario a tali fini. È necessario progettare il sistema di trattamento di dati garantendo la non eccessività di dati raccolti. È pertanto onere del Comune garantire che le attività di sviluppo e realizzazione di nuovi servizi siano condotte solo in seguito ad una formale approvazione da parte del proponente in seguito ad una valutazione dei requisiti espressi, dell'analisi del rischio e dei controlli di sicurezza e protezione dei dati. L'adozione di accorgimenti infatti favorisce una maggiore aderenza ai principi di *Security* e *Privacy by Design*.
Il Comune si impegna ad applicare e attuare la *Privacy-by-Design* e *by Default* in ogni progetto che comporti degli scenari di cambiamento a processi/funzioni/servizi, indipendentemente dalle aree funzionali coinvolte da suddetti cambiamenti.

## 5. DATA PROTECTION IMPACT ASSESSMENT (VALUTAZIONE DI IMPATTO PRIVACY)

La DPIA rappresenta lo strumento guida da seguire in materia di protezione dei dati personali qualora venga identificato un rischio "alto" per i diritti e le libertà degli interessati.
Al fine di promuovere un approccio che consenta la preventiva identificazione dei rischi specifici connessi al trattamento dati, e in ottemperanza a quanto previsto dall'art. 35 del GDPR, risulta necessario, qualora la probabilità di accadimento della minaccia sia ritenuta alta e le conseguenze della minaccia gravi, eseguire il *Data Protection Impact Assessment* (DPIA) sul trattamento dei dati personali previsto nell'ambito del nuovo progetto o della nuova iniziativa coinvolgendo diversi attori ritenuti competenti per legge o per scelta organizzativa dell'Amministrazione (Referenti *Privacy/privacy Officer* , *Information Security IT*, DPO, ecc.).
Le persone responsabili di effettuare la DPIA e i relativi esperti a supporto devono garantire che il processo risulti conforme a tutti i requisiti legislativi, normativi e contrattuali in materia di protezione dei dati.
Nello specifico i soggetti individuati dovranno:
- identificare la legislazione, i regolamenti e i contratti pertinenti applicabili al processo DPIA;
- identificare i *set* di controlli di sicurezza delle informazioni;
- descrivere i controlli già pianificati o esistenti che dovrebbero soddisfare i requisiti di riservatezza;
- utilizzare le informazioni pertinenti presenti in precedenti progetti effettuati.
- Procedere alla stesura della DPIA.

## 6. DATA BREACH

Il Comune in caso di violazione dei dati, ovvero ogni evento che comporti 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, adotta strumenti idonei, ai sensi del GDPR per la gestione del data breach.
Il Titolare, in particolare, *fornisce* al personale del Comune le indicazioni da seguire per una gestione efficace ed efficiente della violazione dei dati trattati.
Il Titolare, di concerto con il DPO, elabora idonea procedura per gestire il processo di rilevazione di un data breach e di valutazione della sua portata per adempiere al obbligo di notifica, entro le 72 ore dal momento in cui viene rilevata, all' Autorità Garante ed agli interessati.
Il comune istituisce apposito registro per la registrazioni delle violazioni dei dati (Registro Data Breach).

## 7.GESTIONE DEI RAPPORTI CON L'AUTORITÀ GARANTE

Nell'ottica di garantire l'efficacia del modello sviluppato e raggiungere i requisiti di *compliance* imposti dalla normativa *Privacy*, risulta necessario prevedere un processo di gestione dei rapporti con l'Autorità Garante che includa almeno:
- la consultazione preventiva (art. 36 del GDPR);

- il riscontro alle richieste dell'Autorità Garante;
- la notifica in caso di violazione dei dati personali;

Con riguardo alla consultazione preventiva ai sensi dell'art. 36 del GDPR, il Titolare del trattamento consulta l'Autorità Garante in via preventiva e qualora, all'esito della valutazione d'impatto sulla protezione dei dati di cui all'art. 35 del GDPR, risulti che il trattamento presenta un rischio elevato in assenza di misure adottate dal Comune.

La comunicazione trasmessa all'Autorità Garante deve contenere almeno:

- la posizione degli attori coinvolti nel trattamento (titolari, contitolari, responsabili, ecc.);
- le finalità e i mezzi del trattamento previsto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
- i risultati della valutazione d'impatto effettuata;
- ogni altra informazione eventualmente richiesta.

L'Autorità Garante può richiedere informazioni relativamente a segnalazioni o ricorsi degli Interessati oppure, nell'ambito di indagini conoscitive, richiedere contributi informativi specifici; inoltre può, anche in occasione delle verifiche ispettive, raccogliere documentazione relativamente alle misure tecniche e organizzative implementate a protezione dei dati personali trattati, documentazione contrattuale, modelli e documenti *privacy* estendendo l'analisi a qualsiasi altro processo, misura o trattamento effettuato da parte del Titolare. Il riscontro alle richieste di informazioni deve essere fornito entro il termine indicato al fine di evitare possibili sanzioni.

## 8. ENTRATA IN VIGORE DEL REGOLAMENTO

Il presente Regolamento entra in vigore decorsi 15 giorni dalla data di pubblicazione all'Albo Pretorio on line da effettuarsi dopo che la deliberazione di approvazione sia divenuta esecutiva.

## 9. NORME ABROGATE

Con l'entrata in vigore del presente regolamento sono abrogate tutte le norme regolamentari con esso contrastanti.

## 10. PUBBLICITÀ DEL REGOLAMENTO

Copia del presente regolamento è pubblicato nell'apposita sezione di Amministrazione trasparente del sito internet istituzionale.

ALLEGATO 1
**Registro dei Trattamenti**

# REGISTRO UNICO DEI TRATTAMENTI (art. 7, c.8, Regolamento comunale)

| **ENTE TITOLARE DEL TRATTAMENTO** | | **Responsabile protezione dati** | |
|---|---|---|---|
| Indirizzo | | Indirizzo | |
| N. telefono | | N. telefono | |
| Mail | | Mail | |
| PEC | | PEC | |
| **Delegato dal Titolare** (eventuale) | | **Registro tenuto da** | |
| Indirizzo | | **Data di creazione** | |
| N. telefono | | **Ultimo aggiornamento** | |
| Mail | | **N. schede compilate** | |
| PEC | | **Prossima revisione** | |

| | TRATTAMENTO | | | | | DATI PERSONALI | | | INTERESSATI | | DESTINATARI | | TRASFERIMENTI | SICUREZZA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| n. ordine | Descrizione | Finalità | Categorie | eventuale diverso Titolare e/o Contitolare (eventuale Rappres.nte) | Responsabile | Categoria | Dati sensibili (SI/NO) | Termine ultimo cancell.ne | Categoria | Consenso (SI/NO) | Categoria | Paesi terzi, org.ni int.li (eventuale) (SI/NO) | Paesi terzi, org.ni int.li (eventuale) | Misure tecniche ed organizzative adottate |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |