



Città di Santa Maria Capua Vetere

(Provincia di Caserta)

DELIBERAZIONE DI CONSIGLIO COMUNALE

N° 29 del 29.05.2025

Oggetto: Modifiche al “Regolamento Comunale relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali” approvato con Deliberazione C.C. n.31 del 27/07/2018.

L'anno duemila venticinque il giorno 29 del mese di maggio alle ore 17:40 presso la Casa Comunale sita in Via Albana (Palazzo Lucarelli) sala delle adunanze comunali del Comune di Santa Maria Capua Vetere, previo recapito di appositi avvisi, si è riunito il Consiglio Comunale, su convocazione del Presidente del Consiglio Comunale, in seduta straordinaria in 2ª convocazione.

Al momento del presente provvedimento, risultano presenti ed assenti i sottototati componenti.

n.	cognome e nome	presente	assente	n.	cognome e nome	presente	assente
	Mirra Antonio (Sindaco)	X					
1	Aveta Raffaele		X	13	Fumante Davide		X
2	Buscetto Daniela	X		14	Graziano Rosario	X	
3	Capitelli Gerardo		X	15	Maffei Alessandro	X	
4	Casino Giuseppe		X	16	Masciandro Roberta	X	
5	Ciarmiello Pasquale	X		17	Mastroianni Salvatore	X	
6	Cipullo Pasquale	X		18	Napolitano Giuseppe		X
7	Crisileo Italo		X	19	Pardi Merola Luigi		X
8	De Lucia Fabio	X		20	Petrella Francesco		X
9	Di Monaco Gaetano	X		21	Sepolvere Anna	X	
10	Di Monaco Giuseppe	X		22	Talento Danilo	X	
11	Di Rienzo Enrico	X		23	Valiante Martino	X	
12	Feola Danilo	X		24	Volpe Giovanna	X	

Partecipa il Segretario Generale del Comune dott.ssa Mariaemilia Lista.

CONSIGLIO COMUNALE

Sentito il Presidente porre in discussione il settimo punto all'o.d.g. (già quinto punto prima dell'inversione dell'o.d.g.) avente ad oggetto: Modifiche al "Regolamento Comunale relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali" approvato con Deliberazione C.C. n.31 del 27/07/2018".

Sentito il Presidente del Consiglio Comunale cedere la parola al Sindaco quale relatore sul punto in questione.

Sentito l'intervento del Sindaco, che sarà riportato nel verbale di seduta, nel quale lo stesso afferma che la proposta di deliberazione in esame è un semplice adeguamento al dettato normativo.

Considerato che non vi sono richieste di intervento e dichiarazioni di voto sull'argomento;

Visto il parere favorevole di regolarità tecnica reso dal responsabile del Settore competente ai sensi del D.lgs. 267/2000;

Sentito il Presidente porre in votazione la proposta di deliberazione che allegata al presente atto ne forma parte integrante e sostanziale;

Con votazione per appello nominale con il seguente esito: Consiglieri presenti 17, assenti 8 (Aveta, Capitelli, Casino, Crisileo, Fumante, Napolitano, Pardi, Petrella), votanti e favorevoli 17

DELIBERA

di approvare, come approva, l'allegata proposta di deliberazione.

Successivamente, con votazione per alzata di mano dall'analogo esito: Consiglieri presenti 17, assenti 8 (Aveta, Capitelli, Casino, Crisileo, Fumante, Napolitano, Pardi, Petrella), votanti e favorevoli 17

DELIBERA

di dotare il presente atto della immediata eseguibilità.



Città di Santa Maria Capua Vetere

Provincia di Caserta

Proposta di Consiglio Comunale

Oggetto: Modifiche al “Regolamento Comunale relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali” approvato con deliberazione C.C. n. 31 del 27/07/2018.

IL DIRIGENTE DEL SETTORE AFFARI ISTITUZIONALI

RICHIAMATO il Regolamento UE 679/2016 e la normativa italiana di armonizzazione (D.Lgs 101 del 10/08/2018 che adegua il Codice Privacy, D.Lgs 196/2003, alle nuove disposizioni europee;

DATO ATTO che il vigente “Regolamento comunale relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali” approvato con deliberazione C.C. n. 31 del 21/07/2018 necessita di alcune modifiche a seguito dell’introduzione di nuove disposizioni normative in materia;

ACQUISITO il parere del Dirigente del Settore Affari Istituzionali in merito alla regolarità tecnica, ai sensi dell’art. 49 T.U.E.L. ;

VISTO il T.U.E.L. 18 agosto 2000, n. 267;

VISTO il vigente Statuto comunale;

PROPONE

1. DI APPROVARE le modifiche al “Regolamento comunale relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali” che si compone di n. 17 articoli, di cui all’ allegato A) che forma parte integrante della presente deliberazione;
2. di DISPORRE che l’efficacia del Regolamento decorre dopo 15 giorni dalla pubblicazione del presente provvedimento all’Albo pretorio on line, ai sensi dell’art. 10 delle preleggi;
3. di DISPORRE la pubblicazione del Regolamento sul sito istituzionale, sez. «Amministrazione Trasparente – Disposizioni generali- atti generali».

IL DIRIGENTE

Dott.ssa Giacomina Giustino



Città di Santa Maria Capua Vetere

Provincia di Caserta

Proposta di Consiglio Comunale

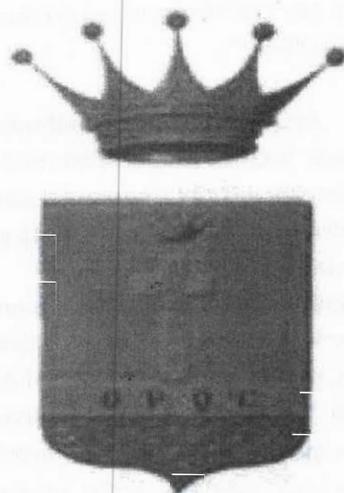
Oggetto: Modifiche al “Regolamento Comunale relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali” approvato con deliberazione C.C. n. 31 del 27/07/2018

PARERE IN ORDINE ALLA REGOLARITÀ TECNICA

Sulla proposta di deliberazione di cui al presente atto, a norma del combinato disposto degli articoli 49, comma 1, e 147 bis, comma 1 del D.Lgs. 18 agosto 2000, n.267 si rende parere favorevole in ordine regolarità tecnica, attestando la regolarità e correttezza dell'azione amministrativa.

Il Dirigente del Settore Servizi alla Persona
Dott.ssa Giacomina Giustino

09/04/2025



Città di Santa Maria Capua Vetere

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

Art. 1 - Oggetto

1. Il presente Regolamento ha per oggetto misure procedurali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento Europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla Protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, che sono eseguiti all'interno dell'organizzazione intesa in ogni sua articolazione del Comune di Santa Maria Capua Vetere (d'ora innanzi indicato come "Comune" o "Ente").

Art. 2 - Finalità del trattamento

1. Il Comune, nell'assolvimento delle proprie finalità istituzionali secondo i principi di trasparenza, efficacia ed economicità, garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il rispetto del diritto alla riservatezza e all'identità personale, nonché delle norme vigenti in materia di protezione e gestione dei dati.
2. L'Ente in adempimento dell'obbligo di comunicazione interna ed esterna e di semplificazione dell'azione amministrativa, favorisce la trasmissione di dati personali e documenti contenenti informazioni di natura personale, tra le banche dati/ archivi del Comune, degli Enti territoriali, degli Enti pubblici, dei gestori e degli incaricati di pubblico servizio operanti nell'ambito dell'Unione Europea, siano essi generati sulla base di un trattamento automatizzato, informatizzato, cartaceo.
3. La trasmissione dei dati personali può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità;
4. Ai fini del presente regolamento, per finalità istituzionali del Comune, si intendono le funzioni ad esso attribuite dalle leggi, dallo statuto e dai regolamenti o per effetto di accordi e/o convenzioni.
5. I trattamenti sono compiuti dal Comune per le seguenti finalità:
 - a) L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Rientrano in questo ambito i trattamenti compiuti per:
 - 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;
 - la gestione dei servizi elettorali, di stato civile, anagrafe, leva militare e di statistica;
 - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione;
 - b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
 - c) l'esecuzione di un contratto con soggetti interessati;
 - d) le specifiche finalità diverse da quelle ai precedenti punti, purché l'interessato esprima il consenso al trattamento;

Art. 3 – Definizioni

1. Ai fini del presente regolamento si intende per:
 - trattamento, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai 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;

- dato personale, qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- dati personali particolari ovvero i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, 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 personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- titolare del trattamento, 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- responsabile del trattamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- responsabile per la protezione dati (RPD), il dipendente della struttura organizzativa del Comune, il professionista privato o impresa esterna, incaricati dal titolare o dal responsabile del trattamento;
- incaricati, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- interessato, la persona fisica cui si riferiscono i dati personali;
- consenso dell'interessato, qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- dato anonimo, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- blocco, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- banca di dati, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- garante, l'autorità preposta al controllo della privacy;
- violazione di dati personali, 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. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
- profilazione, qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- DPIA (Data Protection Impact Assessment), valutazione d'impatto sulla protezione dei dati che è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità e a prevederne i relativi rischi allo scopo di approntare misure idonee ad affrontarli;

2. Ai fini del popolamento del registro del trattamento del Titolare ai sensi dell'art. 30 del GDPR , si intende per:
- **Categorie di trattamento:** raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione, profilazione, ogni altra operazione applicata a dati personali;
 - **categorie di dati personali:** dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale e sociale. Dati inerenti lo stile di vita, situazione economica, finanziaria, patrimoniale, fiscale, dati di connessione (indirizzo IP, login, altro), dati di localizzazione (ubicazione, GPS, GSM, altro);
 - **finalità del trattamento:** esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (quali, per esempio, le funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico), la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica, l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune), adempimento di un obbligo legale al quale è soggetto il Comune, esecuzione di un contratto con i soggetti interessati, altre specifiche e diverse finalità;
 - **misure tecniche ed organizzative:** minimizzazione, cifratura, misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali, procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento, altre misure specifiche adottate per il trattamento di cui trattasi, sistemi di autenticazione, sistemi di autorizzazione; sistemi di protezione (antivirus, firewall, antintrusione e altro) adottati a protezione del trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso, quali per esempio misure antincendio, sistemi di rilevazione di intrusione, sistemi di sorveglianza, sistemi di protezione con videosorveglianza, registrazione accessi, porte, armadi e contenitori dotati di serrature, sistemi di copiatura e conservazione archivi elettronici, altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso, procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
 - **dati particolari (ex sensibili):** dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute, la vita o l'orientamento sessuale, dati genetici e biometrici;
 - **dati giudiziari:** dati relativi a condanne penali e a reati o a connesse misure di sicurezza;
 - **categorie interessati:** cittadini residenti, minori , elettori, contribuenti, utenti, partecipanti al procedimento, dipendenti, amministratori, fornitori, altro.
 - **categorie destinatari:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

Art. 4 – Titolare del trattamento

1. Il Comune di Santa Maria Capua Vetere, rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, è il titolare del trattamento dei dati personali raccolti o meno in archivi/banche dati, automatizzate o non automatizzate (informatizzate o cartacee). Il Sindaco può delegare le relative funzioni al/ai Dirigente/i in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento di dati personali è effettuato in modo conforme al RGPD.
4. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15 e 22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
5. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di PEG, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche;
6. Il Titolare adotta misure, azioni e mezzi appropriati per fornire all'interessato:
 - a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
 - b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non sono stati raccolti presso lo stesso interessato.
7. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 RGPD, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 15.
8. Il Titolare, inoltre, provvede a:
 - a) designare i soggetti designati al trattamento nelle persone dei Dirigenti dei Settori in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;
 - b) nominare il responsabile della protezione dei dati;
 - c) nominare quale responsabile del trattamento i soggetti esterni all'organizzazione dell'Ente, pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione Comunale, che comportino il trattamento di dati personali di interessati dell'Ente, contenuti in banche dati/archivi gestite da tali soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;
 - d) predisporre l'elenco dei responsabili del trattamento dei settori in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.
9. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da Enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
10. Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati,

per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei responsabili del trattamento.

Art. 5 – Responsabile del trattamento

1. Il titolare del trattamento allorquando affidata all'esterno della propria organizzazione un servizio/attività che comporta implicitamente il trattamento di dati personali di interessati del Comune, ricorre unicamente a soggetti in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 7 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.
2. I responsabili del trattamento sono designati mediante un contratto o altro atto giuridico ai sensi dell'art. 28 RGDP anche con decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:
 - la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
 - il tipo di dati personali oggetto di trattamento e le categorie di interessati;
 - gli obblighi ed i diritti del Titolare del trattamento.

Tale disciplina, deve essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun responsabile designato.

3. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
4. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione Europea.
5. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.
6. Il responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.
7. Il responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
8. Il responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione ed in particolare provvede:
 - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;

- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- alla designazione del responsabile per la protezione dei dati (RPD), se a ciò demandato dal Titolare;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art. 6 – Responsabile della protezione dei dati

1. Il Sindaco, con suo provvedimento, nomina il responsabile comunale della protezione dei dati, in funzione delle sue qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di controllo a lui affidati. La nomina ha durata di anni 3.
2. Il responsabile comunale della protezione dei dati può essere scelto fra i dipendenti del Comune oppure all'esterno, qualora tra i dipendenti non vi siano figure professionali idonee. Nel caso in cui il RPD sia interno all'Ente sarà scelto tra i dirigenti o tra i titolari di P.O., se non nominati soggetti designati al trattamento o tra i dipendenti di qualifica non inferiore alla cat. D purché dette figure siano 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 e di assolvere i compiti di controllo a lui affidati.
3. Il Titolare provvede affinché il RPD, se individuato internamente all'Ente, mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione. Nel caso in cui il RPD non sia un dipendente dell'Ente, l'incarico sarà affidato ad un soggetto esterno, persona fisica o giuridica, mediante avviso di selezione pubblica fra soggetti aventi le medesime qualità professionali richieste al dipendente, ossia comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione e di assolvere i compiti di controllo a lui affidati, approfondita conoscenza delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili. I compiti attribuiti al RPD sono indicati in apposito contratto di servizi. La determinazione del compenso è fissata con delibera di Giunta. Il RPD esterno è tenuto a mantenere, a propria cura e spese, la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.
4. L'atto di nomina ed i dati di contatto del responsabile della protezione dei dati sono pubblicati sul sito istituzionale del Comune nella sezione Amministrazione trasparente e comunicati al Garante della protezione dei dati personali.
Il RPD è incaricato dei seguenti compiti:
 - a) informare e fornire consulenza al Titolare in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al soggetto designato al trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, 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 RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare 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 RGPD;
 - 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 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare del trattamento al Garante;
 - f) altri compiti e funzioni a condizione che il Titolare si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.
5. Il Titolare del trattamento assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti che abbiano per oggetto questioni inerenti la protezione dei dati personali;
 - il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
 - il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione.
- Il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.
6. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:
- a) Partecipa alla mappatura delle aree di attività e alla valutazione del grado di rischio in termini di protezione dei dati;
 - b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività incentrandola sulle aree di attività di trattamento che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.
7. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.
8. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il responsabile per la prevenzione della corruzione e per la trasparenza;
 - il responsabile del trattamento;
 - qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
9. Il Titolare del trattamento fornisce al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:
- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;
 - tempo sufficiente per l'espletamento dei compiti affidati al RPD;
 - supporto adeguato in termini di risorse finanziarie, compatibilmente con le risorse finanziarie del bilancio e infrastrutture (sede, attrezzature, strumentazione);
 - comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
 - accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.
10. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti. Il RPD non può essere rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare – nella persona del Sindaco o suo delegato al trattamento (soggetto designato). Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al responsabile del trattamento.

Art. 7 – Sicurezza del trattamento

1. Il Comune di Santa Maria Capua Vetere e ciascun responsabile del trattamento mettono in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono la capacità di assicurare la continua riservatezza, integrità, disponibilità dei sistemi e dei servizi che trattano i dati personali, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Settore cui è preposto ciascun responsabile del trattamento:
 - sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus, firewall, antintrusione, altro);
 - misure antincendio, sistemi di rilevazione di intrusione, sistemi di sorveglianza, sistemi di protezione con videosorveglianza, registrazione accessi, porte, armadi e contenitori dotati di serrature e ignifughi, sistemi di copiatura e conservazione di archivi elettronici, altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

3. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
4. Il Comune di Santa Maria Capua Vetere e ciascun responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
5. I nominativi ed i dati di contatto del Titolare e dei responsabili del trattamento e del responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.
6. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto della normativa vigente in materia di protezione dei dati personali sia europea (Regolamento UE 2016/679 o RGDP) sia nazionale (D.Lgs. 193/2006 e ss.mm.ii.) e in ossequio alle Linee Guida e ai Provvedimenti emanati dall'Autorità Garante.

Art. 8 - Adozione registro delle attività di trattamento

1. Al fine di coordinare le attività oggetto di trattamento, è adottato il "Registro delle attività di trattamento" in allegato A. Con la scheda di trattamento di cui all'allegato 1 al presente Regolamento, si dovrà procedere all'alimentazione e al periodico aggiornamento del registro dei trattamenti.
2. Il registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
 - a) il nome ed i dati di contatto del Comune, del Sindaco e/o del suo delegato ai sensi del precedente art.2, eventualmente del contitolare del trattamento del RPD;
 - b) le finalità del trattamento;
 - c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
 - d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
 - e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
 - f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
 - g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 7.
3. Il registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 4, presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea, secondo lo schema dell'allegato A al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.
4. Il Titolare può decidere di tenere un registro unico dei trattamenti che contiene le informazioni di cui ai commi precedenti e quelle di cui al successivo art. 9, sostituendo entrambe le tipologie di registro dagli stessi disciplinati, secondo lo schema dell'allegato C al presente Regolamento. In tal caso, il Titolare delega la sua tenuta al soggetto a tal fine designato al trattamento come da art. 4 del presente Regolamento sotto la responsabilità del medesimo Titolare. Ciascun Dirigente di Settore quale soggetto designato con riferimento al trattamento di dati personali eseguito nello svolgimento delle attività demandate alla propria area/servizio ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto, ogni elemento necessario alla regolare tenuta ed aggiornamento del registro unico.

Art. 9 – Registro delle categorie di attività trattate

1. Il registro delle categorie di attività trattate da responsabile di cui al precedente art. 5, reca le seguenti informazioni:
 - a) il nome ed i dati di contatto del responsabile del trattamento e del RPD;

- b) le categorie di trattamenti effettuati da ciascun responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, ogni altra operazione applicata a dati personali;
 - c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
 - d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come dal precedente art.7.
2. Il registro è tenuto dal responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema dell'allegato B al presente regolamento.

Art. 10 – Trattamento dei dati personali

1. Le disposizioni del presente regolamento si intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'esterno. L'accesso ai dati personali da parte delle strutture e dei dipendenti del Comune comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale il Comune provvede alla organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitare l'accesso e la fruizione, anche presso le strutture dipendenti.
2. Ogni richiesta di accesso ai dati personali da parte delle strutture e dei dipendenti comunali, debitamente motivata, deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale.
3. Il responsabile della banca dati, specie se la comunicazione concerne dati sensibili, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone.

Art. 11 – trattamenti consentiti

1. Il Comune, di norma, non è tenuto a chiedere il consenso al trattamento dei dati da parte degli interessati.
2. La pubblicazione e la divulgazione di atti e documenti che determinano una "diffusione" dei dati personali, comportando la conoscenza dei dati da parte di un numero indeterminato di cittadini, è legittima solo se la diffusione è prevista da una norma di legge o di regolamento.
3. Prima della pubblicazione di dati personali deve essere valutato se le finalità di trasparenza e di comunicazione possono essere perseguite senza divulgare dati personali.
4. Se risulta possibile occorre citare i dati personali solo negli atti a disposizione degli uffici, richiamati quale presupposto della deliberazione e consultabili solo da interessati e controinteressati oppure utilizzare espressioni di carattere generale, soprattutto nel quadro dell'attività di assistenza e beneficenza, che spesso comporta la valutazione di circostanze e requisiti personali che attengono a situazioni di particolare disagio.
5. Deve essere valutato anche la possibilità di rendere pubblici atti e documenti senza indicare i dati che portino all'identificazione degli interessati.
6. Per attività di comunicazione istituzionale che contemplino l'utilizzo di dati personali, andrà posta particolare attenzione alla necessità di fornire un'adeguata informativa relativa al trattamento e soprattutto andrà valutato se risulti necessaria l'acquisizione, anche successivo, del consenso al trattamento.
7. Negli atti destinati alla pubblicazione o divulgazione i dati che permettono di identificare gli interessati sono riportati solo quando è necessario ed è previsto da una norma di legge, rispettando il principio di proporzionalità, mediante la verifica che tale pubblicazione a fini di trasparenza concerne solo dati pertinenti e non eccedenti rispetto alle finalità perseguite.

8. I sistemi informativi ed i programmi informatici devono essere configurati per ridurre al minimo l'utilizzazione di dati personali e devono prevedere la possibilità di estratti degli atti con l'esclusione dei dati personali in essi contenuti.

Art. 12 – Attività amministrativa

1. L'attività amministrativa del Comune si svolge, principalmente, con l'emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.
2. Per l'attività informatica di cui al comma precedente sono rigorosamente rispettate le norme di cui al codice dell'Amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni.
3. La sicurezza dei dati personali è assicurata anche mediante adeguate soluzioni tecniche connesse all'utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche.

Art. 13 – Trattamento e accesso ai dati sensibili e giudiziari

1. Per l'accesso ai dati sensibili (definiti "particolari" secondo la nuova normativa europea) e giudiziari, con determinazione del responsabile del servizio sono rilasciate autorizzazioni singole per il trattamento dei dati e la manutenzione.
2. L'autorizzazione è limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni assegnate all'incaricato.
3. In attuazione del Regolamento UE 679/2016 le tabelle, raccolte nell'allegato 1 che formano parte integrante del presente regolamento, identificano i tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite.
4. I dati sensibili e giudiziari individuati dal presente regolamento sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'interessato.
5. I dati sensibili o giudiziari non indispensabili, dei quali il Comune, nell'espletamento della propria attività istituzionale, venga a conoscenza, ad opera dell'interessato, comunque, non a richiesta del Comune medesimo, non sono utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Art. 14 – Diritti dell'interessato

1. I soggetti, i cui dati sono contenuti in una banca dati del Comune, hanno il diritto di ottenere, senza indugio:
 - la conferma dell'esistenza o meno di trattamenti di dati che li riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità del trattamento;
 - la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
 - l'aggiornamento, la rettifica ovvero, qualora vi abbiano interesse, l'integrazione dei dati;
 - l'attestazione che le operazioni di cui ai successivi commi 2 e 3 sono state portate a conoscenza dei terzi.
2. L'interessato ha, inoltre, il diritto di opporsi, per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta. L'interessato può esercitare tali diritti con una richiesta al responsabile della banca dati.
L'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

Art. 15 – Valutazioni d'impatto sulla protezione dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la DPIA, si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
 - a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
 - b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
 - c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
 - d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
 - e) trattamenti di dati su larga scala, tenendo conto del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento, volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento, durata o persistenza dell'attività di trattamento, ambito geografico dell'attività di trattamento;
 - f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
 - g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
 - h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
 - i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.
5. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

6. Il responsabile trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
7. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.
8. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
9. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
10. La DPIA non è necessaria nei casi seguenti:
 - se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
 - se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
 - se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
 - se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.
11. Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.
12. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
 - a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi, una descrizione funzionale del trattamento, gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
 - b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
 - delle finalità specifiche, esplicite e legittime;
 - - della liceità del trattamento;
 - dei dati adeguati, pertinenti e limitati a quanto necessario;
 - del periodo limitato di conservazione; - delle informazioni fornite agli interessati;
 - del diritto di accesso e portabilità dei dati;
 - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
 - dei rapporti con i responsabili del trattamento;
 - delle garanzie per i trasferimenti internazionali di dati;
 - consultazione preventiva del Garante privacy;
 - c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

- d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
13. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
14. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.
15. La DPIA deve essere effettuata, con eventuale riesame delle valutazioni condotte, anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 16 Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
- danni fisici, materiali o immateriali alle persone fisiche;
 - perdita del controllo dei dati personali;
 - limitazione dei diritti, discriminazione;
 - furto o usurpazione d'identità;
 - perdite finanziarie, danno economico o sociale.
 - pregiudizio alla reputazione;
 - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatasi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
 - riguardare categorie particolari di dati personali;
 - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
 - comportare rischi imminenti e con un'elevata probabilità di accadimento;
 - impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
6. Il Titolare 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 in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art. 17-Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.
2. Il presente regolamento entra in vigore 15 giorni dalla pubblicazione del presente provvedimento sull'Albo pretorio online, ai sensi dell'art. 10 delle preleggi.

INDICE

Art. 1 – Oggetto

Art. 2 - Finalità del trattamento

Art. 3 – Definizioni

Art. 4 – Titolare del trattamento

Art. 5 – Responsabile del trattamento

Art. 6 – Responsabile della protezione dei dati

Art. 7 – Sicurezza del trattamento

Art. 8 - Adozione registro delle attività di trattamento

Art. 9 – Registro delle categorie di attività trattate

Art. 10 – Trattamento dei dati personali

Art. 11 – trattamenti consentiti

Art. 12 – Attività amministrativa

Art. 13 – Trattamento e accesso ai dati sensibili e giudiziari

Art. 14 – Diritti dell'interessato

Art. 15 – Valutazioni d'impatto sulla protezione dati

Art. 16 Violazione dei dati personali

Art. 17-Rinvio

ALLEGATI:

ALL. 1- SCHEDA DEL TRATTAMENTO

ALL. A- REGISTRO DEL RESPONSABILE DEL TRATTAMENTO

ALL. B- REGISTRO UNICO DELL'ATTIVITA' DI TRATTAMENTO

ALL. C-REGISTRO PARZIALE DELLE ATTIVITA' DI TRATTAMENTO

SCHEDA ATTIVITA' DI TRATTAMENTO
DENOMINAZIONE DEL TRATTAMENTO
DESCRIZIONE DEL TRATTAMENTO
BASE GIURIDICA (fonte normativa)
CATEGORIE DI DATI TRATTATI
FINALITA'
PRINCIPALI OPERAZIONI ESEGUITE [x]

DATI PERSONALI (ex art. 4 Reg. UE 2016/679)	DATI PARTICOLARI (ex art. 9 Reg. UE 2016/679)	DATI GIUDIZIARI (ex art. 10 Reg. UE 2016/679)						
	i dati trattati sono idonei a rivelare: ORIGINE [x] razziale etnica CONVINZIONI [x] APPARTENENZA religiose filosofiche SINDACALE [x] DATI RELATIVI ALLA SALUTE DATI GENETICI [x] DATI BIOMETRICI [x]							
FINALITA'								
FINALITA' DEL TRATTAMENTO	INFORMATIVA	CONSENSO						
	[x] SI [x] NO	[x] SI [x] NO						
1								
2								
3								
4								
5								
6								
7								
8								
PRINCIPALI OPERAZIONI ESEGUITE [x]								
Raccolta	Registrazione	Organizzazione	Conservazione	Modifica	Consultazione	Uso	Comunicazione	Diffusione
			Cancellazione	Distruzione				

--	--

CATEGORIE DI INTERESSATI

--

PERSONALE AUTORIZZATO AL TRATTAMENTO

soggetti che raccolgono i dati personali

--

MODALITA' DI CONSERVAZIONE [x]

Informatizzata

Cartacea

--	--

Strumenti utilizzati

PERIODO DI CONSERVAZIONE

--

TRASFERIMENTO DATI EXTRA UE

NO [x]

SI [x]

PAESI DESTINATARI

CATEGORIE DI DESTINATARI

soggetti ai quali i dati personali sono comunicati

1	
2	
3	

Compilare la parte sottostante soltanto qualora si abbia conoscenza di eventuali misure di sicurezza applicate al trattamento dei dati personali

Misure di Sicurezza	Fisiche	
	Organizzative	
	Logiche	

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

ex art. 30, par. 1, Regolamento UE 2016/679 (General Data Protection Regulation)

TITOLARE DEL TRATTAMENTO

Denominazione	Comune di Santa Maria Capua Vetere
Forma giuridica	Ente Pubblico
Indirizzo/Sede Legale	Via Albana 91, 81055 S. Maria C. V.
P. Iva/ C.F.	00136270618
Numero Telefono	0823 813111
Email	
PEC	protocollo@santamariacv.postecert.it

SETTORE

RESPONSABILE DELLA PROTEZIONE DATI (R.P.D./D.P.O.)

Denominazione	Slalom Consulting srl
Indirizzo/Sede Legale	Via Frosinone, n. 27 - 82037 Telesse Terme (BN)
P. Iva/ C.F.	01757120629
Numero Telefono	0824 277067
Email	dpo@slalomsrl.it
PEC	slalom@pec.net

DATA DI CREAZIONE DEL REGISTRO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

ex art. 30, par. 2, Regolamento UE 2016/679 (General Data Protection Regulation)

RESPONSABILE DEL TRATTAMENTO

Denominazione	Comune di Santa Maria Capua Vetere
Forma giuridica	Ente Pubblico
Indirizzo/Sede Legale	Via Albana 91, 81055 S. Maria C. V.
P. Iva/ C.F.	00136270618
Numero Telefono	0823 813111
Email	
PEC	protocollo@santamariacv.postecert.it

TITOLARE DEL TRATTAMENTO

Denominazione	
Forma giuridica	
Indirizzo/Sede Legale	
P. Iva/ C.F.	
Numero Telefono	
Email	
PEC	

RESPONSABILE DELLA PROTEZIONE DATI (R.P.D./D.P.O.)

Denominazione	Slalom Consulting srl
Indirizzo/Sede Legale	Via Frosinone, n. 27 - 82037 Telesse Terme (BN)
P. Iva/ C.F.	01757120629
Numero Telefono	0824 277067
Email	dpo@slalomsrl.it
PEC	slalom@pec.net

DATA DI CREAZIONE DEL REGISTRO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

DATA AGGIORNAMENTO

REGISTRO DEL TITOLARE DEL TRATTAMENTO

ex art. 30, par. 1, Regolamento UE 2016/679

Cod.	Settore/Cariche	Titolarato	Link a base giuridica	Prestati al trattamento	Organismi di trattamento	Categorie, scopi e finalità (Distribuzione e vendita)	Categorie di interessati	Categorie di dati personali		Data associata alle categorie dei dati trattati	Categorie di dati trattati	Finalità del trattamento (art. 6 del GDPR)	In base a quali giustificazioni della legge per il trattamento internazionale sono i dati personali essere trattati	In base a quali giustificazioni della legge per il trattamento internazionale	Durata di conservazione dei dati (se applicabile)	Misure di sicurezza (tecniche ed organizzative adottate)
								Identificazione	Finalità							
								Identificazione	Finalità							

Il Presidente del
Consiglio Comunale
Sepolvere Anna

F.to _____

Il Segretario Generale
dott.ssa Mariaemilia Lista

F.to _____

Attestato di Pubblicazione

Su attestazione del Messo Comunale, si certifica che copia della presente deliberazione, ai sensi dell'art. 124, I comma, Decreto Legislativo 18/08/2000 n.ro 267 è stata pubblicata all'Albo Pretorio il giorno 10 GIU. 2025 e vi rimarrà pubblicata per 15 giorni consecutivi.

S. Maria Capua Vetere 10 GIU. 2025

Il Messo Comunale

F.to ADRIANO MESSINA

Il Segretario Generale
dott.ssa Mariaemilia Lista

F.to _____

Certificati di esecutività

Si certifica che la presente deliberazione è divenuta esecutiva ai sensi del decreto legislativo del 18/8/2000 n.ro 267 il giorno _____

- Poiché dichiarata immediatamente eseguibile (art. 134, comma 4).
- Essendo decorsi 10 giorni dalla sua pubblicazione (art. 134, comma 3).

S. Maria Capua Vetere _____

Il Segretario Generale
F.to dott.ssa Mariaemilia Lista

Copia conforme all'originale

S. Maria Capua Vetere 10 GIU. 2025

Il Segretario Generale
dott.ssa Mariaemilia Lista

