COMUNE DI SANTA MARIA DELLA VERSA

Provincia di Pavia

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

Approvato dal Consiglio Comunale con deliberazione n. 25 del 30.11.2018

INDICE

A partire dal 25 maggio 2018 è pienamente applicabile il G.D.P.R 679/2016 sulla protezione dei dati personali.

Tale normativa innovando il precedente quadro normativo è basato sul principio di accountability che impone al titolare del trattamento di adottare politiche e attuare misure adeguate per garantire – ed essere in grado di dimostrare – che il trattamento dei dati personali effettuato è conforme al GDPR (art. 5, par. 2).

Questo significa che l'amministrazione dovrà sempre costantemente garantire la conformità di tutte le proprie attività alle regole europee adottando un modello di gestione dei trattamenti dati personali effettuati.

Per effetto della nuova normativa, l'Amministrazione dovrà ripensare a nuove politiche di gestione dei dati personali trattati, passando da una visione statica legata ai formalismi ad una versione dinamica che pone al centro il cittadino, i suoi dati e i conseguenti diritti ora novellati e potenziati in un'ottica di sempre maggior chiarezza e trasparenza.

Da un lato la c.d. "trasparenza proattiva" che si sostanzia nell'obbligo per il titolare di rendere l'informativa, cioè di dare evidenza – senza alcuna specifica richiesta – delle principali informazioni che riguardano il trattamento.

Dall'altro lato la "trasparenza reattiva", impone di riscontrare le richieste dell'interessato e aventi ad oggetto non solo i dati forniti precedentemente dallo stesso, ma anche gli altri dati che il titolare abbia raccolto da altre fonti.

L'adeguamento al principio di trasparenza impone di:

- adeguare e integrare le informative attualmente in uso;
- organizzarsi per riscontrare le richieste di accesso nel termine di trenta giorni dalla ricezione.

Rispetto al codice privacy 196/2003 tuttora in vigore nella sua versione novellata dal D. Lgs 101/2018, sparisce la figura del responsabile interno essendo ora il responsabile solo esterno.

Il titolare del trattamento rimane sempre l'Ente Pubblico nel suo complesso.

In considerazione delle particolari categorie di dati che trattano gli uffici pubblici, gli adempimenti e le attività previste sono sicuramente impegnative e pregnanti.

Per questo motivo, è stato predisposto un piano di adeguamento indivuando all'interno dell'amministrazione un'unità privacy costituita da:

- Segretario comunale
- Responsabile dei servizi demografici
- Responsabile dei servizi finanziari
- Responsabile del servizio tecnico
- Un collaboratore amministrativo

L'unità privacy si occuperà stabilmente dell'adeguamento al GDPR e degli adempimenti da questo previsti (revisione delle informative, registro delle attività di trattamento ecc).

Le fasi del piano di adeguamento prevedono le seguenti fasi:

Fase 1 – Privacy Assessment

Un privacy assessment presuppone una mappatura dei ruoli e dei trattamenti, in conformità alle disposizioni incluse nel GDPR. Devono essere rilevate le informazioni che riguardano le categorie dei dati trattati, le finalità del trattamento, le misure di sicurezza previste per la protezione dei dati, i destinatari delle comunicazioni dei dati e le categorie dei soggetti interessati.

Fase 2 – Organizzazione Privacy

In seguito, si procede con la definizione del modello organizzativo privacy; saranno individuate le figure della Pubblica Amministrazione che sono coinvolte nel trattamento dei dati, dai responsabili ai titolari, per attribuire loro le responsabilità e i ruoli relativi.

Si procederà ad adeguare le informative relative ai vari trattamenti posti in essere dal Comune.

Fase 3 – analisi dei rischi e dpia

Questa fase prevede l'analisi dei rischi che incombono sui dati trattati, analisi che verrà condotta considerando le misure di sicurezza in essere presso l'ammin istrazione comunale.

Si procederà ad eventuale valutazione di impatto.

Fase 4 – Revisione dei processi Privacy

Una volta mappati i trattamenti e i flussi di dati si individeueranno le procedure capaci di definire un sistema di protezione continuativo. Per fare ciò occorrerà sempre effettuare la revisione periodica delle procedure e dei processi privacy.

Fase 5 – Audit Privacy

Saranno effettuati audit Privacy cioè di verifiche degli adempimenti imposti dal GDPR, finalizzate a verificare che siano state adottate tutte le misure organizzative e tecniche previste.

GLOSSARIO REGOLAMENTO

Ai fini del presente Regolamento comunale, si intende per:

- Titolare del trattamento: l'autorità pubblica (il Comune o altro ente locale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali;
- Responsabile del trattamento: il Responsabile di Settore/Servizi oppure il soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento;
- Sub-responsabile del trattamento: il dipendente della struttura organizzativa del Comune, incaricato dal Responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento (elabora o utilizza materialmente i dati personali);

- 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;
- Registri delle attività di trattamento: elenchi dei trattamenti in forma cartacea otelematica tenuti dal Titolare e dal Responsabile del trattamento secondo le rispettive competenze;
- DPIA - Data Protection Impact Assessment – Valutazione d'impatto sulla protezione dei dati: è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali;
- Garante Privacy: il Garante per la protezione dei dati personali che rappresenta l'autorità amministrativa pubblica di controllo indipendente.

Art. 1 - Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27.04.2016, 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, nel Comune di Santa Maria della Versa.

Art. 2 - Titolare del trattamento

1. Il Comune di Santa Maria della Versa (PV), è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco può delegare le relative funzioni ai Responsabili di Settore/Servizi in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati

personali stabiliti dall'art. 5 del 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 a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.

4. Le suddette misure sono definite fin dalla fase di progettazione e sono 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 da 15 a 22 del RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

5. Gli interventi necessari per l'attuazione delle medesime misure sono considerati nell'ambito della programmazione operativa (Documento Unico di Programmazione - DUP), del bilancio di previsione e del Piano Esecutivo di Gestione (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 appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 del RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 del RGPD, qualora i dati personali non stati ottenuti 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 del RGDP, considerati la natura, l’oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

8. Il Titolare, inoltre, provvede a:

a) Individuare una unità privacy che avrà lo scopo di gestire gli adempimenti imposto dal G.D.P.R. 679/2016;

b) nominare il Responsabile della Protezione dei Dati (RPD);

c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell’Amministrazione comunale, relativamente alle banche dati gestite da 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.

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 del 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. 3 - Finalità del trattamento

1. 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. 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, di anagrafe, di leva militare e di statistica;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

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) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 4 Informativa agli interessati

Il Titolare informa gli interessati circa:

- FINALITÀ E BASE GIURIDICA DI TRATTAMENTO
- NATURA OBBLIGATORIA E FACOLTATIVA DEL CONFERIMENTO DEI DATI E CONSEGUENZE DI UN EVENTUALE RIFIUTO
- MODALITA' DI TRATTAMENTO
- TRASFERIMENTO DATI ALL'ESTERO
- TEMPI DI CONSERVAZIONE
- AMBITO DI CONOSCENZA DATI
- COMUNICAZIONE E DIFFUSIONE

- DIRITTI DELL' INTERESSATO
- TITOLARE DEL TRATTAMENTO

Informa altresì circa l'indirizzo del sito web dell'Amministrazione comunale ed il recapito della Segreteria generale presso la quale è consultabile l'elenco aggiornato dei responsabili.

L'informativa prevista dalla legge e dal comma precedente e l'indicazione dei luoghi ove è possibile prenderne visione sono pubblicizzate nella rete civica e presso le segreterie dei Servizi ed Uffici comunali.

I responsabili del trattamento dei dati personali assicurano che la modulistica contenga, anche in sintesi, o abbia allegato un prospetto informativo con gli elementi indicati al comma precedente.

Art. 5 - Responsabile del trattamento

1. Il Titolare del trattamento può avvalersi, per il trattamento di dati, anche sensibili,di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative necessarie, 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.

2. I soggetti di cui al comma 1 sono tenuti a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare.

3. 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, del RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

4. 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. 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.

5. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità edabbia 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.

6. 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, fatta salva la possibilità di affidamento al RDP di cui al successivo art. 8, comma 3;
- all'adozione di idonee misure tecniche e organizzative adeguate a 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 (RPD)

1. Il Responsabile della Protezione dei Dati (in seguito indicato con "RPD"), tenuto conto delle incompatibilità di cui al successivo comma 8, è individuato in un dipendente comunale di categoria professionale non inferiore a "D" in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il Titolare ed il Responsabile del trattamento provvedono affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

2. In assenza di dipendenti in possesso delle suddette qualità professionali il RPD è individuato in un soggetto esterno al Comune scelto tramite procedura ad evidenza pubblica ed in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, all'adeguata conoscenza delle strutture organizzative degli Enti locali e delle norme e procedure amministrative agli stessi applicabili, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. I compiti attribuiti al RPD esterno sono indicati in apposito contratto di servizi.

3. Il RPD esterno è tenuto a mantenere la propria conoscenza specialistica mediante

adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare ed al Responsabile del trattamento.

4. E' possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più Comuni mediante esercizio associato della funzione, nelle forme previste dal T.U. Enti Locali, approvato con D.lgs 18.08.2000, n. 267 e s.m.i.

5. Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento 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 Responsabile del 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 e del Responsabile 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 e/o dal Responsabile del trattamento al Garante;

f) la tenuta dei registri di cui ai successivi artt. 7 e 8, qualora ne venga affidato l'incarico da parte del Titolare del trattamento o del Responsabile del trattamento, ai sensi, rispettivamente, dei citati art. 7, comma 3, e 8, comma 3;

g) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento 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.

6. Il Titolare ed il Responsabile del trattamento assicurano 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 Responsabili di Settore/Servizi 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.

7. 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) procede ad una mappatura delle aree di attività valutandone il 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 che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

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 ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente, 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 Responsabili di Settore/Servizi e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), del bilancio di previsione e del PEG;

- tempo sufficiente per l'espletamento dei compiti affidati al RPD;
- supporto adeguato in termini di infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, di personale;
- 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; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

11. Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

12. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare o al Responsabile del trattamento.

13. 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 Titolare mette in atto misure tecniche ed organizzative adeguate a 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 pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza 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; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate:

- 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.

4. 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.

5. Il Comune si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del RPD sono pubblicati sul sito internet istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

7. Restano in vigore le misure di sicurezza previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico (ex artt. 20 e 22 del D.lgs n. 193/2006).

Art. 8 - Registro delle attività di trattamento

1. 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 Titolare del trattamento e/o del suo delegato ai sensi del precedente art. 2, comma 1, dell'eventualmente 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. 6.

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea, secondo lo schema allegato "A" al presente regolamento a mero titolo esemplificativo; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.

3. Il Titolare del trattamento può decidere di delegare il compito di tenere il Registro al RPD, sotto la responsabilità del medesimo Titolare.

Art. 9 - Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del

medesimo trattamento (DPIA), ai sensi dell'art. 35 del 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, del 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, del 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 del RGDP;

e) trattamenti di dati su larga scala, tenendo conto: del numero di 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.

4. 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.

5. 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.

6. 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.

7. Il RPD monitora lo svolgimento della DPIA.

8. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

9. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o il Settore/Servizio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

10. 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.

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

12. La DPIA non è necessaria nei casi seguenti:

a) 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, del RGDP;

b) 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;

c) 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;

d) 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.

13. Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP 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.

14. 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 e 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.

15. 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.

16. 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.

17. 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. 11 Pubblicità e diffusione dati personali

Il Comune di Santa Maria della Versa, in sede di pubblicazione e diffusione tramite l'albo pretorio informatico e la rete civica di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:

a) sicurezza;

b) completezza;

c) esattezza;

d) accessibilità tramite l'albo pretorio informatico e la rete civica, nel rispetto delle disposizioni del presente Capo;

e) legittimità e conformità ai principi dstabiliti dal G.D.P.R. 679/2016.

Salvo il rispetto degli obblighi di pubblicità legale, gli atti e i provvedimenti amministrativi adottati dagli organi di indirizzo politico e dai dirigenti sono pubblicati sulla rete civica nei casi, con le modalità e per i periodi di tempo espressamente previsti dalle disposizioni di legge vigenti in materia di trasparenza.

La pubblicazione di cui al comma precedente è effettuata nel rispetto delle disposizioni di legge e di regolamento vigenti in materia di protezione dei dati personali. L'Amministrazione adotta le misure organizzative necessarie a rendere non intellegibili i dati personali la cui diffusione non sia espressamente prevista da disposizioni di legge o di regolamento.

È esclusa la diffusione di dati identificativi di persone fisiche nei casi in cui da tali dati sia possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale degli interessati.

Art. 12 - 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.
- decifratura non autorizzata della pseudonimizzazione;
- 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 verificatesi. 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 (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- 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 del 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. 13 – 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.