Comune di San Massimo

Provincia di Campobasso

REGOLAMENTO COMUNALE DI ATTUAZIONE DEL REGOLAMENTO UE N. 679/2016 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Approvato con deliberazione di Consiglio Comunale n. 38 del 28/10/2022

TITOLO I

CAPO I

DISPOSIZIONI GENERALI

ART. 1 - OGGETTO

Al fine di garantire ad ogni persona fisica il diritto alla protezione dei dati personali, il Comune di San Massimo, in attuazione del Regolamento Europeo del 27 aprile 2016 N. 679 (c.d. GDPR), adotta il presente regolamento che disciplina lo svolgimento dei trattamenti di dati personali eseguiti da questo Ente.

Il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito «Regolamento», e del D. Lgs. n. 196/2003 (di seguito, per brevità, Codice della privacy).

Il Comune di San Massimo, sostiene e promuove al suo interno ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla protezione dei dati personali e migliorare la qualità del proprio operato.

Dal momento dell'assunzione del presente regolamento da parte dell'Ente, lo stesso è messo a conoscenza di tutti i dipendenti che si impegnano a prenderne visione ed attenersi alle prescrizioni in esso contenute.

ART. 2 - AMBITO DI APPLICAZIONE

Il Regolamento disciplina il trattamento dei dati personali relativi alle persone fisiche, anche con riguardo alle particolari categorie di dati di cui all'art. 9 del GDPR, da parte di entità terze aventi o meno personalità giuridica e non si applica, quindi, al trattamento dei dati di persone giuridiche.

ART. 3 - DEFINIZIONI

Ai fini del presente regolamento si intende per:

1) **archivio**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
2) **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;
3) **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;
4) **dati particolari**: categoria di dati personali che rivela l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
5) **destinatario**: 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. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
6) **limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

7) **profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali 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;

8) **trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

9) **violazione dei dati personali**: la 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.

ART. 4 – PRINCIPI DA APPLICARE AL TRATTAMENTO DEI DATI PERSONALI

1. Tutte le attività di trattamento di dati personali operate dagli uffici del Comune di San Massimo dovranno osservare i seguenti principi:

a) liceità, correttezza e trasparenza: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) limitazione della finalità: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità;

c) minimizzazione dei dati: i dati personali raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) esattezza: i dati personali raccolti devono essere esatti e, se necessario, aggiornati. Devono essere, inoltre, adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) limitazione della conservazione: i dati personali raccolti devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

f) integrità e riservatezza: i dati personali raccolti devono essere trattati in maniera da garantire un'adeguata sicurezza ivi compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti, dalla perdita, dalla distruzione e dal danno accidentale.

2. Con riferimento ai principi di limitazione della finalità, l'ulteriore trattamento dei dati personali ai fini dell'archiviazione nel pubblico interesse, per la ricerca scientifica o storica o ai fini statistici non è considerato incompatibile con le finalità iniziali.

3. Con riferimento al principio di limitazione della conservazione, i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente ai fini dell'archiviazione nel pubblico interesse, per la ricerca scientifica o storica o ai fini statistici.

ART. 5 - LICEITÀ DEL TRATTAMENTO

4. Il trattamento dei dati è lecito senza il consenso dell'interessato se esso è necessario:

a) all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
b) per adempiere un obbligo legale al quale è soggetto il Titolare del Trattamento;
c) per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
d) per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
e) per il perseguimento del legittimo interesse del Titolare del Trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

5. E' altresì lecito svolgere trattamenti di dati particolari ex art. 9 GDPR qualora essi riguardano dati personali resi manifestamente pubblici dall'interessato o qualora essi:

a) sono necessari per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del Trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
b) sono necessari per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
c) sono effettuati, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religioseo sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
d) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
e) sono necessari per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
f) sono necessari per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;
g) sono necessari per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
h) sono necessari a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

6. Qualora il trattamento dei dati avvenga nella circostanza indicata al precedente punto h) il trattamento dovrà essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato. Tali garanzie dovranno assicurare che siano state predisposte misure tecniche e organizzative, in particolare quelle finalizzate a garantire il rispetto del principio della minimizzazione dei dati. Tali misure dovranno includere l'utilizzo della tecnica della pseudo minimizzazione o di qualsiasi altra tecnica che non permetta più l'identificazione dell'interessato, qualora l'applicazione di tali misure non siano di ostacolo al conseguimento della finalità stabilita.

7. Qualora il trattamento dei dati non avvenga nell'ambito di alcuna circostanza rappresentata ai precedenti comma 1 e 2, esso è lecito solo se l'interessato ha prestato il proprio consenso.

8. Il consenso dovrà essere formulato mediante un atto positivo inequivocabile, con il quale l'interessato manifesta l'intenzione libera, specifica e informata di accettare il trattamento dei dati personali che lo riguardano. Dovranno, inoltre, essere adottate misure tecniche volte a garantirne la verificabilità.

9. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento su di esso basata prima della revoca.

CAPO II
DIRITTI DELL'INTERESSATO

ART. 6 - DIRITTI DELL'INTERESSATO

1. Con riferimento ai dati personali trattati dal Comune di San Massimo, l'interessato può avvalersi del:

a) **diritto di accesso**, ossia avere conferma dell'esistenza o meno di un trattamento di dati personali che lo riguardano e, in caso affermativo, di venire a conoscenza delle caratteristiche del trattamento;

b) **il diritto di rettifica**, ossia la modifica di dati personali inesatti e/o l'integrazione di dati personali incompleti;

c) **il diritto di cancellazione**, ossia la richiesta di immediata cancellazione dei dati personali se ne ricorrono i presupposti normativi;

d) **il diritto di limitazione**, ossia ottenere una limitazione al trattamento dei suoi dati personali;

e) **il diritto alla portabilità dei dati**, ossia ottenere, in caso di trattamenti effettuati con mezzi automatizzati, in formato strutturato i dati personali che lo riguardano al fine di trasferirli presso un'altra organizzazione.

f) **diritto di opposizione**, ossia di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, a trattamenti di dati personali che lo riguardano e svolti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri oppure per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.

g) **diritto di opposizione a processi decisionali automatizzati,** ossia richiedere di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2. Al fine di tutelare i propri diritti l'interessato può proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali ovvero inviare una richiesta scritta al Titolare del Trattamento ovvero inviare una richiesta scritta al Responsabile per la Protezione dei Dati

ART. 7 - INFORMATIVA

1. Ai sensi dell'Art. 13 del GDPR è istituita un'area, all'interno del portale istituzionale del Comune e raggiungibile dalla pagina principale dello stesso, in cui saranno pubblicate le informative mediante le quali gli interessati potranno ottenere informazioni sui trattamenti di dati personali eseguiti dall'Ordine.

2. Per il tramite dell'informativa, che dovrà essere redatta in forma concisa, trasparente, intelligibile e con un linguaggio semplice e chiaro, l'interessato, qualora la raccolta dati avviene presso lo stesso, dovrà essere portato a conoscenza:

a) dell'identità e dei dati di contatto del titolare del trattamento;

b) dei dati di contatto del Responsabile della Protezione dei Dati;

c) delle finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) dei legittimi interessi perseguiti dal Titolare del Trattamento o da terzi, qualora il trattamento si basi sulle circostanze indicate all'articolo 4, comma 1, lettera e);

e) degli eventuali destinatari o delle eventuali categorie di destinatari dei dati personali;

f) dell'eventualità che i dati personali vengano trasferiti a un paese terzo o a un'organizzazione internazionale;

g) del periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

h) dell'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

i) qualora il trattamento sia basato sul consenso espresso dall'interessato, dell'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

j) del diritto di proporre reclamo a un'autorità di controllo;

k) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

l) dell'esistenza di un processo decisionale automatizzato, compresa la profilazione.

3. Per il tramite dell'informativa, che dovrà essere redatta in forma concisa, trasparente, intelligibile e con un linguaggio semplice e chiaro, l'interessato, qualora i dati non siano stati ottenuti presso lo stesso, dovrà essere portato a conoscenza:

a) dell'identità e dei dati di contatto del titolare del trattamento;
b) dei dati di contatto del Responsabile della Protezione dei Dati;
c) delle finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) delle le categorie di dati personali trattati;
e) degli eventuali destinatari o delle eventuali categorie di destinatari dei dati personali;
f) dell'eventualità che i dati personali vengano trasferiti a un paese terzo o a un'organizzazione internazionale;
g) del periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
h) dei legittimi interessi perseguiti dal Titolare del Trattamento o da terzi, qualora il trattamento si basi sulle circostanze indicate all'articolo 4, comma 1, lettera e);
i) dell'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
j) qualora il trattamento sia basato sul consenso espresso dall'interessato, dell'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
k) del diritto di proporre reclamo a un'autorità di controllo;
l) della fonte da cui hanno origine i dati personali e, se del caso, dell'eventualità che i dati provengano da fonti accessibili al pubblico;
m) dell'esistenza di un processo decisionale automatizzato, compresa la profilazione.

CAPO III
TITOLARE DEL TRATTAMENTO, RESPONSABILE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI

ART. 8 - TITOLARE DEL TRATTAMENTO

1. Il Comune di San Massimo è il Titolare del Trattamento dei dati personali raccolti presso i propri uffici e archiviati su supporti sia digitali che cartacei.

2. Il Titolare del Trattamento è responsabile del rispetto dei principi da applicare ai trattamenti di dati personali, con particolare riferimento alle misure tecniche e organizzative da porre in atto al fine di garantire i principi di integrità e riservatezza.

3. Tramite verifiche periodiche il Titolare del Trattamento vigila sulla osservanza, da parte dei designati e dei Responsabili del Trattamento, delle vigenti disposizioni in materia di trattamento dei dati, nonché delle misure tecniche e organizzative impartite attraverso il presente regolamento.

ART. 9 - RESPONSABILE DEL TRATTAMENTO

1. Il Responsabile del Trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del Trattamento, ossia il Comune di San Massimo.

2. Qualora l'affidamento di un servizio o la stipula di una convenzione preveda la presenza della figura del Responsabile del Trattamento dovranno essere individuati unicamente soggetti che presentino garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate a soddisfare il rispetto dei principi di cui all'Art. 3 del presente regolamento e ogni disposizione stabilita della normativa vigente sulla protezione dei dati personali.

3. I rapporti tra il Titolare del Trattamento e i Responsabili del Trattamento dovranno essere stabiliti attraverso contratti o altri atti giuridici, stipulati in forma scritta.

4. Il contratto o altro atto giuridico dovrà identificare la materia disciplinata, la durata, la natura e la finalità, nonché il tipo di dati personali, le categorie di interessati e gli obblighi del Responsabile del Trattamento. In particolare, dovrà obbligare quest'ultimo:

a) a garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
b) ad adottare le misure necessarie a garantire il trattamento in sicurezza di dati personali;
c) ad assistere il titolare del trattamento qualora quest'ultimo sia chiamato a dar seguito alle richieste per l'esercizio dei diritti dell'interessato;
d) a cancellare o restituire tutti i dati personali al termine della prestazione dei servizi e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
e) mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del Trattamento o da un altro soggetto da questi incaricato;
f) a informare immediatamente il Titolare del Trattamento su ogni circostanza che, a suo parere, comporti la violazione del presente regolamento e di ogni altra disposizione in materia di protezione dei dati personali;
g) ad assistere il Titolare del Trattamento nelle procedure finalizzate alla valutazione degli impatti sulla protezione dei dati, fornendo allo stesso ogni informazione di cui è in possesso;
h) a informare il Titolare del Trattamento, senza ingiustificato ritardo, su avvenuti casi di violazione dei dati personali e assistere il Titolare del Trattamento nello svolgimento di ogni procedura consequenziale, quale ad esempio la notifica di violazione all'Autorità Garante per la Protezione dei Dati Personali.

ART. 10 - RESPONSABILE DELLA PROTEZIONE DEI DATI

1. Ai sensi dell'Art. 37 del GDPR è istituita la figura del Responsabile della Protezione dei Dati (c.d. DPO o RPD) che è nominato dal Titolare del Trattamento.

2. Il Responsabile della Protezione dei Dati è la figura professionale incaricata dei seguenti compiti:

a) informare e fornire consulenza al Titolare del Trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il Responsabile della Protezione dei Dati può indicare al Titolare 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 GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare del Trattamento;
c) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
d) cooperare con l'Autorità Garante per la Protezione dei Dati Personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento.

3. La figura del Responsabile della Protezione dei Dati è incompatibile con chi determina le finalità o i mezzi del trattamento. In particolare, risultano con la stessa incompatibili:

a) il responsabile per la prevenzione della corruzione e per la trasparenza;
b) la figura del responsabile del trattamento.

4. Il Responsabile della Protezione dei Dati 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.

5. Il Responsabile della Protezione dei Dati non può essere rimosso o penalizzato dal Titolare del Trattamento per l'adempimento dei propri compiti nel rispetto della normativa applicabile. Con particolare riguardo al disposto dell'art. 38 GDPR.

6. Ferma restando l'indipendenza nello svolgimento di detti compiti, il Responsabile della Protezione dei Dati riferisce direttamente al rappresentante legale pro tempore del Titolare del Trattamento o suo delegato.

ART. 11 - REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

1. Ai sensi dell'Art. 30 del GDPR è istituito il Registro delle Attività di Trattamento che identifica tutti i trattamenti di dati personali operati dal Comune di San Massimo.

2. Il Registro delle Attività di Trattamento, accessibile sotto la responsabilità del Titolare del Trattamento, dai Dirigenti e Responsabili della P.O., dovrà riportare i dati di contatto del Comune e del Responsabile della Protezione dei Dati, e inoltre per ogni trattamento eseguito le seguenti informazioni:

a) le finalità del trattamento;
b) i dati di contatto di un eventuale contitolare 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 e organizzative adottate articolo 12

ART. 12 - VALUTAZIONE DEGLI IMPATTI SULLA SICUREZZA

1. Ai sensi dell'art. 35 del GDPR il Comune attuerà la valutazione degli impatti sulla sicurezza (c.d. DPIA) per ogni trattamento che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

2. Fermo restando quanto indicato dall'art. 35 del GDPR, verrà condotta una DPIA nel caso in cui un trattamento ricada in almeno due delle seguenti circostanze:

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 particolari;
e) trattamenti di dati su larga scala;
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'Ordine, 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.

3. Qualora le risultanze di una PIA indicassero l'esistenza di un rischio residuale elevato, il trattamento oggetto di valutazione potrà essere eseguito solo dopo la consultazione con l'Autorità Garante per la Protezione dei Dati Personali.

4. Il Titolare del Trattamento consulta l'Autorità Garante per la Protezione dei Dati Personali 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 e alla sanità pubblica.

5. La documentazione prodotta a seguito di una PIA sarà tenuta in formato digitale, acquisita al protocollo e posta in conservazione sostitutiva.

6. Il Responsabile della Protezione dei Dati sovrintende all'esecuzione di una DPIA e segnala al Titolare del Trattamento l'insorgere di ogni eventuale problematica che ne possa ostacolare la corretta gestione.

TITOLO II
MISURE TECNICHE ED ORGANIZZATIVE PER LA PROTEZIONE DA TRATTAMENTI NON AUTORIZZATI O ILLECITI, DALLA PERDITA, DALLA DISTRUZIONE E DAL DANNO ACCIDENTALE

CAPO I
MISURE ORGANIZZATIVE

ART. 13 - LINEE GUIDA GENERALI

1. Il trattamento di dati personali dovrà essere eseguito soltanto:
   a) per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti attualmente in vigore nei singoli uffici;
   b) per esigenze di tipo operativo e gestionale;
   c) per ottemperare ad obblighi di legge;
   d) per finalità di programmazione operativa;
   e) per dare esecuzione ad un servizio o ad una o più operazioni concorsualmente convenute.

2. Nell'esecuzione di un trattamento dovranno essere raccolti i soli dati personali necessari al raggiungimento della specifica finalità.

3. Le informazioni trattate dagli uffici del Comune di San Massimo dovranno essere opportunamente cancellate o distrutte nei casi in cui:
   a) non siano più utili al raggiungimento delle finalità istituzionali;
   b) siano relative alla cessazione per qualsiasi causa di trattamenti di dati personali non più necessari o siano eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
   c) gli scopi per le quali sono state raccolte e trattate non siano più determinati, espliciti e legittimi oppure siano diventate incompatibili con tali scopi;
   d) risultino scaduti i termini legittimi di conservazione anche con riferimento al tempo necessario agli scopi per i quali sono stati raccolti o successivamente trattati, siano essi determinati da norme di legge generali e/o di settore (ad es. dieci anni per la conservazione delle scritture contabili) oppure dalle finalità per le quali i dati sono stati raccolti o in relazione alle quali devono essere conservati (ad es. contenziosi);
   e) l'interessato ne richieda la cancellazione nell'esercizio dei propri diritti di cui all'Art. 4 del presente regolamento.

4. Il Responsabile della Protezione dei Dati, di cui all'Art. 7 del presente regolamento, dovrà essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   a) il Responsabile della Protezione dei Dati dovrà essere invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti il trattamento di dati personali;
   b) il Responsabile della Protezione dei Dati deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea.

5. Al Responsabile della Protezione dei Dati dovrà essere fornito il supporto necessario per assolvere ai compiti attribuiti e per accedere ai dati personali e ai trattamenti. In particolare viene assicurato il supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e degli organi collegiali, nonché l'accesso ai settori funzionali del Comune di San Massimo.

ART. 14 - COMUNICAZIONE DEI DATI PERSONALI

1. La comunicazione e la diffusione dei dati personali trattati dal Comune di San Massimo a soggetti pubblici, privati oppure a enti pubblici economici sono ammesse in presenza di specifiche leggi o disposizione normative.

2. Ad eccezione delle ipotesi di trasferimento di dati tra enti pubblici o necessari per indagini di Pubblica Sicurezza è esclusa la messa a disposizione o la consultazione di dati in blocco o la ricerca per nominativo di tutte le informazioni contenute nelle banche dati, senza limiti di procedimento o di settore.

3. Sono escluse dalle previsioni del precedente comma 2 le liste elettorali.

ART. 15 - SOGGETTI DESIGNATI AL TRATTAMENTO

1. Sono soggetti designati al trattamento i Dirigenti/Responsabili P.O. e in quanto tali sono autorizzati a eseguire, per conto del Comune di San Massimo, le attività di trattamento di dati personali necessarie allo svolgimento dei procedimenti propri dell'ufficio di competenza.

2. I Dirigenti/Responsabili P.O. sovrintendono, altresì, a che i trattamenti di dati personali, che saranno svolti all'interno del proprio ufficio di competenza, avvengano nel rispetto delle disposizioni del presente regolamento.

3. Dirigenti/Responsabili P.O. hanno facoltà di nominare, tra i soggetti che operano alle dipendenze Comune di San Massimo, ulteriori designati al trattamento, ossia ulteriori soggetti che nel proprio ufficio di competenza sono autorizzati a svolgere attività di trattamento dei dati personali. In tale caso, i Dirigenti e Responsabili P.O., dovranno sovrintendere sull'osservanza della normativa sulla privacy da parte degli uffici di propria competenza. In particolare, devono, per conto del Titolare del Trattamento, nominare quale persona designata e quindi autorizzata al trattamento dei dati personali, ogni soggetto che, nel rispetto dell'assetto organizzativo, opera sotto l'autorità del Comune di San Massimo, e tratta, necessariamente, dati personali per lo svolgimento delle proprie mansioni. La designazione deve essere formulata compatibilmente alle mansioni assegnate al dipendente e fornendo adeguata formazione e opportune istruzioni scritte. Di tali designazioni dovrà esser posto a conoscenza il Titolare del Trattamento nella persona del legale rappresentante p.t.

4. I soggetti designati al trattamento devono garantire la massima riservatezza, nonché il rispetto delle disposizioni del presente regolamento e in particolare l'applicazione dei principi di cui all'art. 3 del presente regolamento e dei diritti dell'interessato di cui all'art. 4 del presente regolamento.

5. I soggetti che trattano dati personali per conto del Comune di San Massimo rispondono per i danni cagionati al patrimonio e alla reputazione di questo Ente a seguito della violazione delle disposizioni contenute sia nel presente regolamento che nella vigente normativa in materia di tutela dei dati personali.

ART. 16 - TENUTA DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

1. I Dirigenti/Responsabili P.O., relativamente ai trattamenti svolti nei propri uffici di competenza, redigono il Registro delle Attività di Trattamento, di cui all'Art. 8 del presente regolamento, e lo aggiornano ogni qual volta si renda necessario dar luogo a un nuovo trattamento di dati personali.

2. Il Registro della Attività di Trattamento dovrà essere soggetto al processo di revisione annuale durante il quale i Dirigenti/Responsabili P.O. dovranno operare una verifica dei contenuti con particolare riferimento a eventuali dismissioni di trattamenti di dati personali o evoluzioni delle misure tecnico organizzative implementate.

3. Il Responsabile della Protezione dei Dati sovrintende al processo di iniziale stesura, successivi aggiornamenti e revisioni del Registro delle Attività di Trattamento e segnala al Titolare del Trattamento l'insorgere di ogni eventuale problematica che ne possa ostacolare la corretta gestione.

4. Il Titolare del Trattamento trasmette al Responsabile della Protezione dei Dati il Registro delle Attività dei Trattamenti che viene formato:

a) al termine del processo di iniziale stesura;
b) qualora si determini un nuovo aggiornamento;
c) al termine del processo di revisione annuale.

5. Il Registro delle Attività di Trattamento è tenuto in formato digitale, è acquisito al protocollo e posto in conservazione sostitutiva.

ART. 17 - TENUTA DELLE INFORMATIVE

1. I Dirigenti/Responsabili P.O., relativamente ai trattamenti svolti nei propri uffici di competenza, redigono le informative di cui all'Art. 7del presente regolamento, e apportano le necessarie rettifiche ogni qual volta il corrispondente trattamento di dati personali subisce una modifica nelle sue caratteristiche principali.

2. 1. I Dirigenti/Responsabili P.O. sovrintendono, altresì, alla pubblicazione delle stesse nella corrispondente sezione istituita all'interno del portale istituzionale del' Ente.

3. Il Responsabile della Protezione dei Dati sovrintende alla tenuta delle informative redatte dal Comune di San Massimo e segnala al Titolare del Trattamento l'insorgere di ogni eventuale problematica che ne possa ostacolare la corretta gestione.

ART. 18 -RAPPORTI CON I RESPONSABILI DEL TRATTAMENTO

1. Qualora l'affidamento di un servizio o la stipula di una convenzione preveda la presenza della figura del Responsabile del Trattamento, di cui all'Art. 9 del presente regolamento, ossia di un soggetto terzo che esegue un trattamento di dati per conto del Comune di San Massimo, è compito dei Dirigenti/Responsabili P.O. ovvero di chiunque altro soggetto che per conto di questo Ente ha facoltà di determinare l'affidamento o stipulare la convenzione, di individuare unicamente soggetti economici che presentino garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate a soddisfare il rispetto dei principi di cui all'Art. 4 del presente regolamento e ogni disposizione stabilita dalla normativa vigente sulla protezione dei dati personali.

2. E' compito altresì dei Dirigenti/Responsabili P.O. ovvero di chiunque altro soggetto che per conto di questo Ente ha facoltà di determinare l'affidamento o stipulare la convenzione di disciplinare i rapporti con i Responsabili del Trattamento attraverso contratti o altri atti giuridici così come indicato ai punti 3 e 4 dell'Art. 9 del presente regolamento.

ART. 19 - REGISTRI DI INVENTARIO DEI DISPOSITIVI TECNOLOGICI E DEI SOFTWARE AUTORIZZATI

1. Ai sensi di quanto disposto dall'Agenzia per l'Italia Digitale attraverso la circolare N. 2/2017 e ogni ulteriore provvedimento successivo, sono istituiti il registro di inventario dei dispositivi tecnologici e il registro dei software autorizzati.

2. Il registro di inventario dei dispositivi tecnologici dovrà indicare tutte le risorse hardware attive operanti all'interno della struttura informatica del Comune di San Massimo e per ognuna di essa riportare le seguenti informazioni:

a) Denominazione del dispositivo;
b) Funzione del sistema;
c) Numero seriale;
d) Indirizzo IP assegnato;
e) Ufficio assegnato.

3. Il registro dei software autorizzati dovrà indicare i software autorizzati a operare all'interno della struttura informatica del Comune di San Massimo e per ognuno di essi riportare:

a) la denominazione del software;
b) la casa produttrice;
c) la versione del software
d) l'eventuale contratto di servizio per l'erogazione di tale software in modalità SaaS;
e) la eventuale risorsa cloud impiegata

ART. 20 - TENUTA DEI REGISTRI DELL'INVENTARIO DEI DISPOSITIVI TECNOLOGICI E DEI SOFTWARE AUTORIZZATI

1. I registri di inventario dei dispositivi tecnologici attivi e dei software autorizzati di cui al precedente articolo sono tenuti dal soggetto a cui fa capo la responsabilità dei sistemi informativi, il quale dovrà provvedere all'iniziale stesura e ai successivi aggiornamenti, che dovranno aver luogo ogni qual volta nuovi dispositivi

vengono introdotti nel sistema informatico e ogni qual volta si ha la necessità di adottare nuovi software necessari allo svolgimento delle funzioni istituzionali.

2. Il soggetto a cui fa capo la responsabilità dei sistemi informativi dovrà eseguire annualmente una verifica di corrispondenza tra i contenuti dei due registri e i dispositivi tecnologici attivi e i software effettivamente operanti all'interno della struttura informatica del Comune di San Massimo.

ART. 21 - VIOLAZIONE DEI DATI PERSONALI

1. I designati al trattamento dei dati personali e i Responsabili del Trattamento dovranno notificare al Titolare del Trattamento e al Responsabile per la Protezione dei Dati il verificarsi di ogni evento di violazione dei dati personali trattati dal Comune di San Massimo, ossia il verificarsi di eventi che causano trattamenti non autorizzati o illeciti, perdita, distruzione e danno accidentale dei dati.

2. Al verificarsi di ogni evento di violazione, il Titolare del Trattamento, previa consultazione del Responsabile per la Protezione dei Dati, provvederà a notificare l'accaduto all'Autorità Garante per la Protezione dei Dati Personali qualora si ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati quali:

a) danni fisici, materiali o immateriali alle persone fisiche;
b) perdita del controllo dei dati personali;
c) limitazione dei diritti, discriminazione;
d) furto o usurpazione d'identità;
e) perdite finanziarie, danno economico o sociale.
f) corruzione del sistema di anonimizzazione dei dati;
g) pregiudizio alla reputazione;
h) perdita di riservatezza dei dati personali protetti da segreto professionale.

3. La notifica, di cui al precedente comma, avverrà entro le 72 ore dal momento in cui il Titolare del Trattamento è venuto a conoscenza dell'evento di violazione.

4. Se il rischio per i diritti e le libertà degli interessati coinvolti dall'evento di violazione di dati personali è elevato, allora questi ultimi saranno informati, senza ingiustificato ritardo, circa la natura della violazione verificatasi.

5. I rischi per i diritti e le libertà degli interessati saranno considerati "elevati" quando la violazione può:

a) coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
b) riguardare categorie particolari di dati personali;
c) comprendere dati che possono accrescere ulteriormente i potenziali rischi (dati di localizzazione, finanziari, relativi alle abitudini e preferenze, etc.);
d) comportare rischi imminenti e con un'elevata probabilità di accadimento (rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito, etc.);
e) impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (utenti deboli, minori, soggetti indagati, etc.).

6. Gli eventi di violazione dei dati personali trattati dal Comune di San Massimo saranno documentati all'interno del Registro degli Eventi di Data Breach, che, oltre ai riferimenti temporali legati all'accaduto, riporta le circostanze a esso relative, le conseguenze e i provvedimenti adottati.

7. Il Registro degli Eventi di Data Breach sarà tenuto in formato digitale, acquisito al protocollo e posto in conservazione sostitutiva.

CAPO II
MISURE TECNICHE

ART. 22 - TRATTAMENTI DISGIUNTO DEI DATI PARTICOLARI

1. Il trattamento dei dati particolari è soggetto a gestione disgiunta, ossia:

a) l'insieme dei dati personali che identificano una persona dovrà essere trattato separatamente dall'insieme dei dati particolari a essa collegati;
b) il collegamento tra le due tipologie di insiemi avviene attraverso l'utilizzo di codici identificativi atti a impedire l'immediata riconducibilità.

2. L'adozione di tecniche di crittografia e di ogni altro strumento offerto dalla tecnologia corrente, che rendono l'intero insieme dei dati particolari non comprensibili/intelligibili a persone non autorizzate, sostituisce l'obbligo del trattamento disgiunto di cui al precedente punto.

3. Le regole di cui ai precedenti punti sono applicate a ogni trattamento di dati particolari, sia che esso avvenga su supporto cartaceo che digitalmente.

ART. 23 - TRATTAMENTI ESEGUITI MEDIANTE L'UTILIZZO DEI DOCUMENTI IN FORMATO CARTACEO

1. I documenti in formato cartaceo che contengono dati personali dovranno essere conservati in archivi ciechi e dotati di serratura.

2. I documenti in formato cartaceo che contengono dati personali dovranno essere consultati solo all'interno degli uffici dell'Ente non accessibili al pubblico. In caso di allontanamento, anche temporaneo, dalla postazione di lavoro dovranno essere poste in essere tutte le misure necessarie a evitare che soggetti non autorizzati possano accedere ai dati personali contenuti nei documenti in consultazione.

3. Le attività di stampa, fotocopia o acquisizione ottica di documenti contenenti dati personali dovranno essere svolte nel rispetto del principio di riservatezza, ossia evitando che soggetti non autorizzati possano visualizzare il contenuto dei documenti oggetto di trattamento. Al termine dell'attività il documento oggetto di trattamento dovrà essere rimosso dai dispositivi di stampa, fotocopia o acquisizione ottica.

ART. 24 - GESTIONE DEI DISPOSITIVI TECNOLOGICI E DEI SOFTWARE

1. E' fatto divieto di installare sulle postazioni fornite in dotazione qualsiasi software, soggetto a tutela autoriale, contenuto in dischetti, DVD-ROM e altri dispositivi removibili, o direttamente scaricato da Internet, senza la "licenza d'uso commerciale", *shareware* o *open source* senza autorizzazione del Titolare del Trattamento.

2. E' fatto divieto di utilizzare gli strumenti forniti in dotazione, nelle componenti sia hardware che software, in modo improprio o per fini personali.

3. All'interno della struttura informatica del Comune di San Massimo è consentito esclusivamente l'utilizzo di dispositivi tecnologici e software autorizzati, ossia dei dispositivi tecnologici e dei software elencati nei registri di inventario di cui all'Art. 16 del presente regolamento.

4. Il soggetto a cui fa capo la responsabilità dei sistemi informativi provvede alla rimozione dei dispositivi non autorizzati e dei software non autorizzati o comunque non necessari allo svolgimento delle funzioni istituzionali.

ART. 25 - CONTROLLO DEGLI ACCESSI AI DISPOSITIVI E AI SOFTWARE

1. L'accesso alle postazioni di lavoro, alle unità server, ai dispositivi di rete configurabili, ai software, alle risorse cloud e ai software dovrà avvenire attraverso l'utilizzo di sistemi di identificazione, autenticazione e autorizzazione del soggetto che opera su di essi.

2. Qualora sia adottata la password come elemento di autenticazione essa dovrà:
a) avere una lunghezza non inferiore a 8 caratteri oppure, nel caso in cui il sistema non lo dovesse prevedere, di lunghezza pari al massimo consentito;
b) essere cambiata almeno ogni 6 mesi;
c) contenere, ove possibile, almeno un numero e un carattere speciale;
d) essere diversa dalle almeno ultime due precedentemente utilizzate;
e) non contenere riferimenti che permettano un agevole riconducibilità all'utente o ad ambiti noti;
f) non essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet.

3. E' vietato divulgare ad altri le credenziali personali di accesso. Il titolare delle credenziali è responsabile di tutte le azioni e le funzioni svolte per il tramite delle sue credenziali. A tal fine egli in caso di allontanamento, anche temporaneo, dalla postazione di lavoro dovrà attivare la funzionalità di blocco dell'elaboratore sia attraverso gli strumenti messi a disposizione dal sistema operativo (ad esempio CTRL+ALT+CANC), nonché dai sensori biometrici eventualmente disponibili.

4. Le utenze dotate di privilegi di amministrazione di una postazione di lavoro o di una unità server sono utilizzate esclusivamente per dar luogo ad attività di gestione straordinaria delle componenti hardware e software. L'utilizzo ordinario di una postazione di lavoro o di una unità server deve essere effettuato mediante l'accesso con utenze dotate di privilegi limitati.

5. Le utenze dotate di privilegi di amministrazione definite per ogni postazione di lavoro, unità server, dispositivi di rete configurabili e software dovranno essere riportate nel registro delle password che sarà custodito dal responsabile del sistema informativo.

ART. 26 - GESTIONE DELLE POSTAZIONI DI LAVORO E DELLE UNITÀ SERVER E DELLE RISORSE CLOUD

1. E' vietato, all'interno della struttura informatica del Comune di San Massimo, l'utilizzo di postazioni di lavoro e unità server non dotati di software atti a rilevare la presenza e bloccare l'esecuzione di malware (c.d. antivirus). Detti software dovranno essere aggiornabili, nella conoscenza delle impronte virali, in maniera automatico.

2. E' vietato, all'interno della struttura informatica del Comune di San Massimo, l'utilizzo di postazioni di lavoro e unità server su cui operano sistemi operativi non aggiornati o non più aggiornabili. Laddove applicabile l'aggiornamento dei sistemi operativi dovrà essere eseguito in maniera automatico.

3. Il soggetto a cui fa capo la responsabilità dei sistemi informativa di verifica trimestralmente la necessità di operare sui dispositivi di rete l'aggiornamento firmware, procedendo in tal senso quando necessario. Esegue altresì la medesima operazione di verifica con la medesima periodicità per ogni postazioni di lavoro e unità server su cui operano sistemi operativi non aggiornabili in maniera automatica.

4. In caso di malfunzionamento dell'elaboratore in uso, che possa far sospettare la presenza di un virus, malware, cryptolocker, keylogger o strumenti di controllo remoto pur se legittimi ma non autorizzati direttamente dall'utente o dall'organizzazione stessa, è fatto obbligo di:

a) sospendere ogni operazione;
b) contattare immediatamente il soggetto a cui fa capo la responsabilità dei sistemi informativi;
c) chiudere il sistema e le relative applicazioni.
d) consegnare il dispositivo di proprietà dell'organizzazione al responsabile dei sistemi informativi;

5. La copia dei dati personali trattati dal Comune di San Massimo su supporti di memorizzazione di massa esterni nonché risorse cloud diverse da quelle messe a disposizione dall'organizzazione è consentita solo se necessaria per lo svolgimento delle funzioni istituzionali. In tal caso dovranno essere adottati sistemi per la crittografia dei dati, o ogni ulteriore misura disponibile a livello tecnico, affinché questi siano resi non comprensibili né intelligibili a persone non autorizzate.

6. Qualora venga meno la possibilità di adottare i sistemi per la criptazione dei dati di cui al comma precedente, i supporti di memorizzazione di massa esterni che contengono dati personali non potranno lasciare la sede ospitante gli uffici, dovranno essere utilizzati esclusivamente all'interno di quest'ultima e dovranno essere custoditi con diligenza e conservati in armadi o contenitori muniti di serratura.

ART. 27 - COMUNICAZIONI MEDIANTE RETE

1. L'utilizzo della rete Internet e dei servizi accessibili per il suo tramite è consentito solo se necessario per lo svolgimento delle funzioni istituzionali. Sono vietati comportamenti che possano arrecare danno alla reputazione e al patrimonio del Comune di San Massimo.

2. Il trattamento dei dati personali attraverso la rete Internet dovrà aver luogo solo attraverso l'utilizzo di comunicazioni non in chiaro, ossia comunicazioni che adottano, nello scambio dei dati, i protocolli crittografici, le tecnologie di *blockchain* o ogni altra tecnologia superiore.

3. L'accesso alla infrastruttura del Comune di San Massimo mediante tecnologia wireless è consentito solo se necessaria per lo svolgimento delle funzioni istituzionali. In tal caso dovranno essere adottati sistemi di identificazione e autorizzazione dei terminali mediante tecniche di filtraggio del MAC address, virtualizzazione delle schede di rete ovvero sistemi di identificazione, autenticazione e autorizzazione dell'utente, nonché ogni ulteriore misura di livello superiore consentita dalla tecnologia corrente.

4. Le attività di accesso da remoto alle postazioni di lavoro, alle unità server e ai dispositivi di rete sono consentite solo se eseguite mediante l'utilizzo di connessioni protette e sotto il controllo e il monitoraggio del soggetto a cui fa capo la responsabilità dei sistemi informativi.

ARTI. 28 - UTILIZZO DEL SERVIZIO DI POSTA ELETTRONICA, DEI SERVIZI DI MESSAGGISTICA, DEI SERVIZI SOCIAL E DELLE RISORSE CLOUD

1. L'utilizzo della posta elettronica è consentito solo se necessario per lo svolgimento delle funzioni istituzionali. Sono vietati comportamenti che possano arrecare danno alla reputazione e al patrimonio del Comune di San Massimo.

2. L'account di posta elettronica è uno strumento gestito dall'Ente ed è conferito in uso ai dipendenti, collaboratori e cariche istituzionali per l'esclusivo svolgimento delle mansioni lavorative e istituzionali affidate.

3. Ad uno stesso soggetto possono essere assegnate più caselle di posta elettronica, indirizzi anche disgiunti dalla propria casella personale che possono anche essere condivise con altri utenti dello stesso ufficio o di altri uffici, nei limiti del perseguimento di fini istituzionali e di miglioramento oggettivo dei servizi offerti all'utenza.

4. Attraverso le caselle gli utenti rappresentano pubblicamente l'Ente e per questo è fatto obbligo di utilizzare la posta elettronica in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine dell'Ente.

5. Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica affidata e devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- prestare ai contenuti della corrispondenza ricevuta e non aprire allegati o selezionare hyperlink testuali contenuti in e-mail di dubbia provenienza o ricevute nell'ambito di un contesto avulso da quello lavorativo. In tali casi dovranno non aprire il messaggio e segnalare immediatamente l'accaduto al responsabile del sistema informativo;
- rispondere alle e-mail pervenute solo da mittenti conosciuti.

6. Non è consentito l'invio automatico della posta ricevuta su account istituzionale verso un indirizzo di e-mail privato anche durante i periodi di assenza.

7. In caso di assenza improvvisa o prolungata ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio ovvero per motivi di sicurezza del sistema informatico, il Titolare del Trattamento, per il tramite del soggetto l'amministratore di sistema, potrà accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file. Di tale attività sarà redatto apposito verbale e informato il soggetto interessato alla prima occasione utile.

8. In caso di interruzione del rapporto di lavoro, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 (trenta) giorni da quella data ed entro 90 (novanta) giorni si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Ente si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie finalità istituzionali.

9. Salvo l'utilizzo di appositi strumenti di cifratura i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto è fatto obbligo di valutare con attenzione l'invio di informazioni contenenti dati personali che potranno essere trasmessi se:

a) il destinatario è certo;
b) il destinatario è autorizzato a entrare in possesso dei dati personali.

10. Fermo restando l'applicazione di quanto disposto al precedente punto, è fatto, altresì, obbligo di adottare sistemi per la cifratura dei contenuti qualora le informazioni trasmesse attraverso la posta elettronica contengano dati particolari.

11. L'utilizzo dei sistemi di messaggistica istantanea, di trasferimento dei dati o di ogni ulteriore sistema di trasferimento dei dati o di memorizzazione dei dati in cloud è regolamentato dalle medesime norme applicabili ai servizi di posta elettronica. E' fatto divieto utilizzare detti sistemi ove non prevedano tecnologie di crittografia *end-to-end* per la trasmissione di documenti e dati dell'organizzazione, contenenti o meno dati ritenuti sensibili, senza preventiva autorizzazione espressa del Responsabile del Trattamento dei dati o di un suo delegato.

12. L'utilizzo delle risorse cloud o dei servizi SaaS diversi da quelli ufficialmente messi a disposizione da parte dell'organizzazione deve essere espressamente autorizzato dal Responsabile del Trattamento dei dati o di un suo delegato.

ART. 29 - PROCEDURE DI BACKUP DEI DATI

1. Sono adottate procedure volte a eseguire le copie di backup dei dati contenuti all'interno delle unità server e all'interno delle singole postazioni di lavoro, delle risorse mobili e di tutte le risorse cloud disponibili nell'organizzazione.

2. Le procedure di backup dovranno essere eseguite quotidianamente, mediante l'utilizzo di procedure/software che ne garantiscono l'automatizzazione.

3. Il responsabile del sistema informativo sovrintende sulla corretta esecuzione delle procedure di backup e in particolare verifica semestralmente il corretto funzionamento delle procedure di recovery.

ART. 30 - DISTRUZIONE DEI DATI

1. I supporti di memorizzazione di massa (hard disk, DVD, CD, etc.) destinati allo smaltimento dovranno essere oggetto di preventiva distruzione fisica attraverso sistemi di punzonatura, deformazione meccanica o apertura dell'involucro protettivo con danneggiamento delle superfici atte alla memorizzazione.

2. I supporti di memorizzazione di massa destinati al reimpiego dovranno essere oggetto di preventiva cancellazione dei dati che dovrà avvenire mediante l'utilizzo di software di wiping.

3. Le risorse memorizzate in cloud verranno cancellate definitivamente, compatibilmente con le tecnologie in essere al momento dell'esigenza e in tempi e modalità compatibili con le *policy* sottoscritte con il fornitore di servizi, nonché della vigente legislazione nazionale ed europea applicabile ai servizi cloud e SaaS.

CAPO III
VIOLAZIONI E RESPONSABILITÀ

ART. 31 - RESPONSABILITÀ IN CASO DI VIOLAZIONE DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

1. Il mancato rispetto delle disposizioni previste dal presente Regolamento comporta la violazione degli obblighi previsti dalla normativa sulla protezione dei dati personali ed espone il Titolare del Trattamento a rischi sul piano delle responsabilità e delle sanzioni a livello civile, amministrativo e, nei casi più gravi, anche penale.

2. La violazione delle disposizioni previste dal presente regolamento e dalla normativa sulla protezione dei dati personali da parte dei soggetti designati al trattamento dei dati per conto del Comune di San Massimo rende possibile contestare il fatto e infliggere i relativi provvedimenti disciplinari previsti dal C.C.N.L. applicato, nonché a fronte di danni economici, la richiesta del conseguente risarcimento.

ART. 32 - RINVIO

1. Per quanto non previsto nel presente regolamento, si applicano le disposizioni stabilite dalla normativa in materia di tutela delle persone fisiche con riguardo alla protezione dei dati personali, con particolare riferimento alle previsioni contenute nel Regolamento Europeo 2016/679 e nel Codice della Privacy.

2. Il presente regolamento sarà aggiornato a seguito di ulteriori modifiche alla vigente normativa in materia di tutela delle persone fisiche con riguardo alla protezione dei dati personali.