COPIA WEB
Deliberazione **N. 17**
In data **26.03.2019**
Prot. N. **5167**

COMUNE DI ROSSANO VENETO

PROVINCIA DI VICENZA

Verbale di deliberazione del Consiglio Comunale

Sessione ordinaria Convocazione 1ª Seduta pubblica

OGGETTO:

REGOLAMENTO COMUNALE PER LA PROTEZIONE DEI DATI PERSONALI.

L'anno **duemiladiciannove** addì **VENTISEI** del mese di **MARZO** presso la sede municipale.
Convocato dal Sindaco Martini Morena mediante lettera d'invito prot. n. 4007 del 20/03/2019**,** fatta recapitare a ciascun consigliere, si è oggi riunito**,** il Consiglio Comunale sotto la presidenza del Sindaco MARTINI Dott.ssa Morena e l'assistenza del Segretario Comunale Reggente ZANON Dott. Giuseppe.
Fatto l'appello, risulta quanto segue:

	PRESENTI	ASSENTI
1. BATTAGLIN Helga	*	
2. BERTON Chiara	*	
3. BERTON Davide	*	
4. BIANCHIN Cristina	*	
5. CENCI Andrea	*	
6. GALVAN Giulia		*
7. GANASSIN Paola	*	
8. LANDO Doris	*	
9. MARCON Andrea	*	
10. MARTINI Morena	*	
11. PEGORARO Davide	*	
12. TREVISAN Gilberto		*
13. ZONTA Marco	*	

Presenti N. 11 Assenti N. 2

Il Sindaco**, MARTINI Dott.ssa Morena**, assume la presidenza.

PROPOSTA DI DELIBERAZIONE

OGGETTO: "REGOLAMENTO COMUNALE PER LA PROTEZIONE DEI DATI PERSONALI".

IL CONSIGLIO COMUNALE

PREMESSO:

- che il Parlamento ed il Consiglio europeo in data 27.4.2016 hanno approvato il Regolamento UE 679/2016 (GDPR - *General Data Protection Regulation)* relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;
- che il testo del Regolamento, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, è divenuto definitivamente applicabile in via diretta in tutti i Paesi UE;
- che il Garante per la protezione dei dati personali ha emanato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali che intende offrire un panorama delle principali problematiche che i soggetti pubblici;
- che le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy;
- che appare necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questo Ente di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;
- che il Comune di Rossano Veneto non dispone di un testo normativo rispettoso dei principi e delle norme introdotti dal predetto Regolamento europeo e che tale regolamento ha reso obsolete le previgenti fonti normative, anche di rango regolamentare;
- che è stato predisposto un testo normativo, che si allega alla presente proposta di deliberazione, in conformità ai principi espressi dal Regolamento UE 679/2016 (GDPR - *General Data Protection Regulation)* ed in aderenza alle indicazioni operative fornite dal Garante per la protezione dei dati personali;

VISTI:

- la L. 241/1990;
- il D.lgs 193/2006;
- il Regolamento UE 679/2016 (GDPR- General Data Protection Regulation);
- il D.lgs 267/2000 ed i pareri resi ai sensi dell'art. 49 del medesimo decreto legislativo;

DELIBERA

di approvare il "REGOLAMENTO COMUNALE PER LA PROTEZIONE DEI DATI PERSONALI", secondo il testo che si allega.

Sulla suestesa proposta di deliberazione sono stati acquisiti i seguenti pareri ai sensi dell'Art. 49 del D.Lgs n. 267 del 18/08/2000.

VISTO, si esprime parere favorevole in ordine alla regolarità tecnica.

Il Responsabile Area Affari Generali
f.to FERRARO Dott. Adriano

VISTO, si esprime parere favorevole in ordine alla regolarità contabile.

Il Responsabile Serv. Contabile e Gestione delle Entrate
F.to PERTILE Rag. Luisa Lorena

COMUNE DI
ROSSANO VENETO

Regolamento comunale per la protezione dei dati personali

Indice

TITOLO I – I RESPONSABILI DEL TRATTAMENTO

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 n. 679 del 27 aprile 2016, relativo alla protezione delle persone fisiche (RGPD) con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati.

Art. 2 Titolare del trattamento

1. Il Comune di Rossano Veneto, rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, 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 a Responsabile di Posizione Organizzativa in possesso di adeguate competenze.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dal RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dal RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
4. Il Titolare adotta misure appropriate per fornire all'interessato:
a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
5. 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, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.
6. Il Titolare, inoltre, provvede a:
a) designare i Responsabili del trattamento nelle persone dei Responsabili di Posizioni Organizzative in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;
b) nominare il Responsabile della protezione dei dati;
c) nominare quale Responsabile del trattamento i soggetti 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;
d) predisporre l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.
7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
8. 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, stabilite dalla fonte normativa che li disciplinano:
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

b) l'adempimento di un obbligo legale al quale è soggetto il Comune;
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 Responsabile del trattamento

1. Il Responsabile di Posizione organizzativa è nominato unico Responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile unico deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative, volte a garantire che i trattamenti siano effettuati in conformità al RGPD.
2. I dipendenti del Comune, Responsabili del trattamento, sono designati, di norma, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:
- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi ed i diritti del Titolare del trattamento.

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun responsabile designato.
3. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
4. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28 RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
5. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.
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.
6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
7. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali, 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.5 Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato in un professionista scelto tramite procedura ad evidenza pubblica.
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:

- svolgimento di una DPIA;
- metodologia da adottare nel condurre una DPIA;
- salvaguardie da applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
- conclusioni della DPIA;

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;
L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.
2. 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 Posizioni Organizzativa 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.
3. 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.
4. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili (in relazione alle dimensioni organizzative del Comune):
- 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.
5. Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuitigli.
6. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare od al Responsabile del trattamento.

TITOLO II - SICUREZZA DEL TRATTAMENTO

Art. 6 Sicurezza del trattamento

1. Il Comune di Rossano Veneto e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative idonee 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 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 dal Servizio cui è preposto ciascun Responsabile del trattamento:
- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione);
- 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 di Rossano Veneto e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. I nominativi ed i dati di contatto del Titolare, dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente.

Art. 7 Funzionamento delle risorse informatiche

1. Le risorse informatiche tracciano una serie di eventi di sistema per attività amministrative, manutentive e/o di sicurezza, che variano a seconda della tipologia delle risorse stesse.
2. Il tracciamento di tali eventi non è generalmente oggetto di rilevazione da parte del Responsabile del Trattamento. Qualora, per necessità manutentive o di gestione della sicurezza si renda necessario rilevare e/o registrare gli eventi tracciati di una risorsa specifica, tali trattamenti verranno preventivamente segnalati al personale aziendale nelle modalità indicate nei successivi paragrafi.

Art. 8 Utilizzo delle Postazioni di lavoro

1. Il personal computer (PC), affidato al dipendente è uno strumento di lavoro.
2. È vietato l'uso del PC per ragioni e finalità personali.
3. Non è consentito installare programmi, senza l'autorizzazione Responsabile del Trattamento.
4. Non sono consentite la duplicazione e l'installazione abusiva di software, nonché l'uso di programmi diversi da quelli messi a disposizione dall'Ente stesso.
5. Il PC viene consegnato all'utente con una configurazione coerente con le misure organizzative e di sicurezza impostate dall'Ente stesso: non è consentito all'utente di modificare le caratteristiche impostate sulla postazione stessa, salvo preventiva autorizzazione scritta dell'Amministratore di sistema.
6. Il PC deve essere spento prima di lasciare l'ufficio o in caso di assenze prolungate dall'ufficio, salvo specifica disposizione dell'Amministratore di sistema e/o a seguito di pianificazione dello spegnimento automatico. In ogni caso, l'utente che si allontana dalla postazione deve adottare cautele per bloccarne l'uso.
7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente il responsabile del Trattamento nel caso in cui vengano rilevati virus.
8. Non è consentito l'utilizzo di giochi o altre applicazioni di tipo ludico anche se comprese nel sistema operativo installato.
9. Non sono permesse, a meno di specifiche e documentate autorizzazioni le seguenti attività:

a) caricare, memorizzare, pubblicare, diffondere, distribuire, tramite risorse dell'Ente documenti, informazioni, immagini, filmati in generale, ed in particolare:

- a carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso nei confronti dei minori, contrario all'ordine pubblico, diffamatorio o che contenga contenuti illeciti penalmente o civilmente riconducibili a categorie qui non espressamente indicate;
- pregiudizievoli per le risorse dell'Ente e per l'integrità e la conservazione dei dati dell'Ente stesso;
- pregiudizievoli per l'immagine e il buon nome dell'Ente all'esterno dell'Ente;

b) accedere a server web trattanti materie o soggetti ricadenti nelle categorie sopra elencate; tenere comportamenti che possano indurre taluno ad effettuare invii di materiale rientrante nelle tipologie sopra elencate; laddove l'utente si trovi a ricevere anche contro il suo volere tali materiali, è tenuto a informare il Responsabile del Trattamento e attenersi alle sue istruzioni circa il trattamento di tali materiali;
c) utilizzare le risorse dell'Ente con fini di molestia, minaccia o comunque violando le norme di legge in vigore;
d) caricare o trasmettere, con volontà, archivi o programmi contenenti virus o dati alterati;
e) manomettere sistemi o archivi in maniera tale da inficiare la riservatezza, la disponibilità e/o l'integrità dei dati;
f) utilizzare le risorse dell'Ente in modo da consentire a soggetti non abilitati l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla Legge e dai Regolamenti.
10. Le attività sopra elencate possono avere conseguenze di natura penale ed originano in capo al trasgressore tutte le responsabilità previste dalla Legge.

Art. 9 Utilizzo dei supporti mobili e PC portatili

1. Tutti i supporti magnetici riutilizzabili (dischetti, cassette, secure-drive, cd, dvd, chiavi e dischi esterni USB) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da soggetti non incaricati.
2. E' assolutamente vietato l'utilizzo di supporti esterni per la custodia e il salvataggio dei dati: tutte le informazioni utilizzate per lo svolgimento delle funzioni istituzionali devono essere salvate sui server dedicati.
3. E' consentito l'utilizzo di chiavette USB, purché:

- i supporti magnetici contenenti dati sensibili e giudiziari non siano essere portati all'esterno della sede comunale, all'interno della quale, devono comunque essere custoditi in archivi chiusi a chiave;
- ove sia necessario portare dati sensibili e giudiziari all'esterno, sia acquisita l'autorizzazione del Responsabile del Trattamento;

4. E' consentito l'utilizzo di macchine fotografiche digitali per lo svolgimento delle attività lavorative, a condizione di comunicarne al Responsabile del Trattamento l'eventuale connessione a PC comunali per il riversamento delle fotografie, il quale assisterà in caso di necessità gli uffici per la prima installazione di applicativi di interconnessione.

5. L'utente è Responsabile delle attrezzature informatiche portatili assegnategli dal Responsabile del Trattamento e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
6. Ai portatili si applicano le regole di utilizzo previste per i PC connessi alla rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
7. Non è consentito l'utilizzo sul PC di nessun dispositivo di memorizzazione o comunicazione, se non con l'autorizzazione scritta del Responsabile del Trattamento.

Art. 10 Utilizzo della rete locale LAN e rete territoriale WAN
L'acquisizione, l'installazione, la manutenzione, l'amministrazione e l'accesso a sistemi di rete LAN, WAN e WIRELESS facenti parte del sistema informativo comunale è di esclusiva competenza del Titolare del Trattamento.

Art. 11 Utilizzo delle risorse condivise
1. Al fine di garantire la disponibilità dei dati e un'efficace politica di backup, gli utenti devono salvare su cartelle di rete tutti i file di lavoro ed astenersi dal salvarli sul disco locale della postazione di lavoro.
2. Le cartelle/unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità, nemmeno per brevi periodi.
3. Sulle cartelle/unità di rete vengono svolte regolari attività di amministrazione e backup.
4. Le password di ingresso alla rete ed ai programmi sono personali: è assolutamente vietato entrare nella rete e nei programmi con altri nomi utente.
5. Il Responsabile del Trattamento può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza, sia sui PC degli incaricati sia sui server.
6. I Responsabili del Trattamento dovranno effettuare la periodica, almeno ogni 6 mesi, pulizia degli archivi attuando:
- la cancellazione dei file obsoleti ed inutili;
- la verifica della nomenclatura dei file;
- l'eliminazione delle archiviazioni ridondanti, che dovranno comunque essere evitate.

7. Per la trasmissione di file all'interno dell'Ente è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo. Le cartelle di scambio devono essere tenute in ordine, eliminando i file non più necessari anche al fine di non consentire il trattamento dei dati a persone non espressamente incaricate.
8. Gli utenti dovranno effettuare la stampa dei dati solo se strettamente necessaria e dovranno ritirarla prontamente dai vassoi delle stampanti comuni.
9. Il collegamento alla rete comunale di personal computer portatili o di attrezzature informatiche non di proprietà del Comune di Rossano Veneto è vietato.

Art. 12 Acquisizione software
Sulle postazioni è consentita l'installazione esclusiva delle seguenti categorie di software:
- software commerciale dotato di licenza d'uso;
- software gestionale realizzato specificatamente per l'Amministrazione comunale dalle ditte specializzate nel settore della P.A.;
- software realizzato specificatamente dagli organi centrali della Pubblica Amministrazione o Enti nazionali;
- software gratuito (freeware) e shareware prelevato dai siti internet, solo se espressamente autorizzato dal Responsabile del Trattamento

Art. 13 Acquisizione hardware e Servizi con impatto sui sistemi informatici
1. L'acquisizione di materiale hardware o di qualsiasi dispositivo che interagisca con la rete e/o la strumentazione informatica comunale o possa avere un impatto con essi devono essere sempre preventivamente valutati ed autorizzati in collaborazione col Responsabile del Trattamento, al fine di garantire la stabilità dei sistemi, la compatibilità degli hardware con gli stessi, malfunzionamenti, cadute prestazionali o altri problemi alla sicurezza.
2. Le modalità di acquisizione dei dispositivi dovranno rispettare le vigenti disposizioni in tema di contratti pubblici.
3. Qualora nell'esercizio di una funzione amministrativa sia prevista la fornitura di software accessorio alla gestione/erogazione di un servizio, l'ufficio competente provvede a consultare il Responsabile del Trattamento nelle fasi preliminari del processo di acquisizione per la corretta definizione delle caratteristiche del software, affinché lo stesso risulti:
- compatibile con il sistema informatico comunale,
- conforme alle misure di sicurezza adottate dall'Ente con particolare riguardo alla sicurezza degli accessi

- certificato per l'installazione sulle macchine in dotazione al Comune (server e pc)
- installato correttamente

4. Qualora venga affidata all'esterno la gestione di dati comunali per l'erogazione di servizi, l'ufficio competente deve concordare preventivamente con il Responsabile del Trattamento le modalità e i formati con cui questi dati devono essere scambiati sia in ingresso che in uscita e le condizioni di consegna dei dati al termine del rapporto di collaborazione.

Art. 14 Gestione delle password e degli accessi

1. Per garantire un'adeguata protezione dei dati personali, ad ogni utente vengono fornite delle credenziali di accesso a sistemi informatici, applicativi gestionali e siti internet pertinenti con le proprie specifiche attività lavorative. Le credenziali di accesso sono personali e devono essere gestite con cautela dagli utenti.
2. L'utente deve utilizzare sempre una password quando viene richiesto dalla procedura, avendo cura che nessuno ne venga a conoscenza.
3. Nel caso di accesso a sistemi remoti in cui l'accesso a dati personali o sensibili sia protetto da password, è severamente vietato usare un profilo di accesso condiviso con altri utenti: ogni utente che deve accedere a tali sistemi dovrà necessariamente disporre di un proprio profilo personale a garanzia della riservatezza dei dati trattati e della tracciabilità delle operazioni effettuate.
4. Le password del dominio e degli applicativi, salvo impossibilità dovute all'obsolescenza del software, devono essere modificate ogni 3 mesi, devono essere formate da almeno una minuscola, almeno una maiuscola e almeno un numero o carattere speciale; e non devono contenere riferimenti agevolmente riconducibili all'incaricato.
5. Nel caso in cui si sospetti che una password abbia perso la segretezza, l'utente provvederà ove possibile a modificarla personalmente, altrimenti provvederà a modificarla con il supporto dell'Amministratore di sistema.
6. Non è consentito utilizzare il profilo personale di altri soggetti per connettersi al dominio o agli applicativi. Qualora l'utente venisse a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia al Responsabile del Trattamento.
7. Le password non devono essere riutilizzate.

Art. 15 Attività di backup

1. Sono oggetto di attività di salvataggio centralizzato su supporti magnetici o ottici:
    - i file salvati sulle cartelle/unità di rete;
    - il registro di sistema del server;
    - i file di log di sistema del server;
    - le banche dati di applicativi ed i relativi file di sistema;
    - il contenuto delle caselle di posta elettronica gestite dal server.
2. Gli elementi sopra indicati vengono salvati sistematicamente ogni notte di una giornata lavorativa.
3. I dati che risiedono sulle postazioni PC non sono soggetti a operazioni di backup centralizzato.

Per quanto riguarda gli archivi localizzati sulle postazioni di lavoro, l'attività di backup verrà svolta dagli incaricati con gli strumenti messi a disposizione localmente dal Servizio Informatico.

Art. 16 Attività e strumenti di assistenza remota

1. Per finalità di carattere manutentivo sono attivi presso l'Ente strumenti di connessione e assistenza remota che consentono ai manutentori di connettersi alle postazioni di lavoro con lo scopo di assistere gli utenti e fornire supporto in tempo reale nella risoluzione di problematiche di carattere informatico.
2. Gli strumenti utilizzati manifestano esplicitamente la connessione alla postazione da parte dei manutentori: l'utente dovrà consentire tramite autorizzazione verbale o informatica l'intervento remoto.
3. Gli interventi di assistenza remota sulle postazioni da parte di operatori esterni per attività manutentive, detti interventi dovranno comunque essere preventivamente concordati con il Servizio Informatico e da esso autorizzati di volta in volta.

Art. 17 Posta elettronica

1. La casella di posta elettronica, assegnata dall'Ente all'utente, è uno strumento di lavoro.
2. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
3. Qualsiasi attività istituzionale realizzata tramite utilizzo di posta elettronica deve essere svolta con l'esclusivo utilizzo di caselle registrate sotto il dominio di posta istituzionale dell'Ente o tramite caselle di posta elettronica certificata registrate dall'Ente stesso.
4. E' fatto divieto di utilizzare le caselle di posta elettronica comunale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione da parte del Responsabile del Trattamento per esigenze di lavoro.
5. E' inoltre da evitare ove possibile l'invio di messaggi con allegati di grandi dimensioni al fine di non causare sovraccarichi al sistema informativo e nuocere all'efficacia della comunicazione.
6. La casella di posta deve essere tenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

7. Per la trasmissione di file all'interno dell'Ente è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo.
8. E' vietato inviare mail con allegati contenenti file eseguibili.
9. L'utente che riceva messaggi sospetti di richiesta di password o altre informazioni oppure di invito a svolgere operazioni sulla propria postazione di lavoro di cui non è certa la provenienza, dovrà segnalarlo immediatamente al Responsabile del Trattamento prima di effettuare qualsiasi azione.
10 Al fine di garantire la continuità di servizio di posta esterna, sono previste le seguenti modalità per la gestione delle assenze, programmate o non, degli operatori preposti alla lettura dei messaggi di una specifica casella di posta:

- attivazione di un risponditore automatico che segnali la temporanea indisponibilità dell'utente preposto alla lettura della casella;
- nomina di un vicario appositamente incaricato che si occuperà della lettura dei messaggi di posta elettronica;

11 E' vietato utilizzare client di posta elettronica differenti da quelli installati e configurati dal tecnico informativo, incaricato dal Titolare del Trattamento.

Art. 18 Internet
1. Il collegamento ad Internet è uno strumento messo a disposizione per i soli scopi di lavoro: è proibita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza per cui va assolutamente evitato l'utilizzo personale dello stesso.
2. Pertanto, viene attivato un filtro che blocca l'accesso ai siti ritenuti palesemente non pertinenti con le attività istituzionali..
3. Qualora, per lo svolgimento della attività istituzionali, un utente necessiti di accedere a un sito scartato dai sistemi di filtraggio, potrà richiedere l'accesso a tale sito al Responsabile del Trattamento che ne assumerà la responsabilità.
4. E' fatto assoluto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato dai siti internet, se non espressamente autorizzato dal Responsabile del Trattamento.
5. E' tassativamente vietato qualsiasi genere di transazione privata in campo finanziario ivi comprese le operazioni di remote banking, acquisti on-line e simili.
6. E' tassativamente vietata ogni forma di registrazione e connessione a siti i cui contenuti non siano legati all'attività lavorativa.
7. E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat-line, di blog, di bacheche elettroniche e in generale di strumenti di social network anche utilizzando pseudonimi (o nicknames), esclusi gli strumenti autorizzati per esigenze di lavoro.
8. A fini statistici, di qualità del servizio e di sicurezza, l'occupazione di banda generata dal traffico internet e dallo scambio di posta elettronica è soggetta a periodiche verifiche e controllo da parte dell'Ente sotto forma di dati aggregati ed anonimi.
9. Qualora i sistemi di sicurezza segnalino delle potenziali criticità che possano minare l'integrità dei dati e la stabilità del sistema stesso, potranno essere effettuati dei controlli sulla navigazione internet. 10. Tali controlli saranno preventivamente segnalati al personale e si opererà secondo stadi successivi:

- controlli generici sulle pagine visitate, senza che vengano tracciati gli utenti che le visitano;
- controlli aggregati sulle pagine visitate con suddivisione del traffico effettuato per aree;
- controlli specifici sulle pagine visitate, con tracciamento dell'indirizzo IP da cui si effettua la visita o dell'utente che la effettua.

11. Il tracciamento specifico verrà effettuato solo qualora il tracciamento generico e quello aggregato non abbiano consentito di risolvere le criticità riscontrate e verrà comunque nuovamente segnalato in forma preventiva agli utenti.

Art. 19 Sicurezza generale e perimetrale
1. Presso l'Ente è attivato un sistema di sicurezza perimetrale a difesa dei sistemi e dei dati comunali, che traccia eventi che possono essere indizio di minacce informatiche. Il sistema è soggetto a procedure di aggiornamento automatico per quanto riguarda la lista e le caratteristiche delle minacce.
2. Qualora il sistema attivato rilevi delle minacce a specifici indirizzi IP interni delle postazioni di lavoro, il Responsabile del Trattamento verificherà le cause dell'intrusione rilevata insieme all'utente/utenti che abitualmente utilizza/utilizzano la postazione, con l'obiettivo di comprendere la natura dell'intrusione e prevenire eventuali danni.
3. Una volta individuate le cause dell'evento rilevato, verranno adottati provvedimenti correttivi, con segnalazione al Titolare dei trattamenti di eventuali violazioni alle regole indicate nel presente regolamento.

Art. 20 Attività dell'Amministratore di Sistema
1. S'intende per Amministratore di sistema qualsiasi soggetto le cui funzioni di gestione ed amministrazione di

sistemi informatizzati rendano ad esso tecnicamente possibile l'accesso, anche fortuito, a dati personali; in questa definizione rientrano pertanto le funzioni tecnicamente definite di Amministratore di sistema (system administrator), Amministratore di base di dati (database administrator) o Amministratore di rete (network administrator).
2. L'Amministratore di sistema è designato dal Titolare in forma scritta.
3. Fra le funzioni dell'Amministratore di sistema, sia esso interno all'Ente che esterno, vi possono essere:

- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare e/o coordinare interventi di manutenzione hardware per i dispositivi di competenza;
- effettuare interventi di manutenzione software su sistemi operativi e applicativi di competenza;
- coordinare e sovrintendere l'operato di eventuali tecnici esterni all'Amministrazione (nel caso di Amministratore interno);
- coordinare a livello operativo la gestione e la distribuzione dei profili di accesso e delle password degli utenti del sistema e/o dei sottosistemi di competenza nel rispetto delle normative relative alla protezione dei dati personali;
- gestire le password di amministrazione di sistema o dei sottosistemi di competenza;
- collaborare con i responsabili del trattamento dei dati personali per l'organizzazione delle politiche di sicurezza;
- informare il Responsabile dei sistemi informatici e/o il Titolare sulle non corrispondenze con le norme di sicurezza e su eventi di sicurezza rilevanti.

4. Le funzioni di Amministrazione di Sistema possono essere svolte dal Responsabile della Protezione.

TITOLO III – IL TRATTAMENTO DEI DATI

Art. 21 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;
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;
2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato, presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea, secondo lo schema allegato A al presente Regolamento.
3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.
4. Il Titolare può decidere di tenere un Registro unico dei trattamenti che contiene le informazioni di cui ai commi precedenti e quelle di cui al successivo, sostituendo entrambe le tipologie di registro dagli stessi disciplinati, secondo lo schema allegato C al presente Regolamento. In tal caso, il Titolare delega la sua tenuta ad un solo Responsabile del trattamento, ovvero può decidere di affidare tale compito al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Art. 22 Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Responsabile, reca le seguenti informazioni:
a) il nome ed i dati di contatto del Responsabile del trattamento;
b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale.
2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema allegato B al presente regolamento.
3. Il Responsabile del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.

Art. 23 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 RGDP. La DPIA è una procedura che permette di realizzare e dimostrare la legittimità 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.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.
5. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. L'Amministratore di sistema, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.
6. 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.
Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
7. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35 RGDP;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

8. 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.
9. 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.
10. 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.
11. 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. 24 Violazione dei dati personali
1. Per violazione dei dati personali 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, 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 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.

Titolo IV – DISPOSIZIONI FINALI

Art. 25 Entrata in vigore

1. Il presente regolamento entra in vigore il giorno in cui diviene esecutiva la relativa delibera di approvazione. Esso abroga ogni altra disposizione incompatibile con le sue statuizioni.
2. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

ALLEGATI
A) Registro attività di trattamento

REGISTRO ATTIVITA' DI TRATTAMENTO (art. 30, c.1, GPRD)

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

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

B) Registro categorie di attività di trattamento

REGISTRO CATEGORIE DI ATTIVITA' DI TRATTAMENTO (art. 30, c.2, GPRD)			
ENTE TITOLARE DEL TRATTAMENTO		**Responsabile del trattamento**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
		Registro tenuto da	
		Data di creazione	
		Ultimo aggiornamento	
		N. schede compilate	
		Prossima revisione	

	TRATTAMENTO				TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Categorie	eventuale diverso Titolare e/o Contitolare (eventuale Rappres.nte)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

C) Registro unico dei trattamenti

REGISTRO UNICO DEI TRATTAMENTI (art. 7, c.8, Regolamento comunale)			
ENTE TITOLARE DEL TRATTAMENTO		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Registro tenuto da**	
Indirizzo		**Data di creazione**	
N. telefono		**Ultimo aggiornamento**	
Mail		**N. schede compilate**	
PEC		**Prossima revisione**	

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

Il Sindaco pone in votazione la suestesa proposta di deliberazione già illustrata e discussa nel precedente punto, **che viene approvata con voti favorevoli unanimi n. 11**, legalmente espressi da n. 11 consiglieri presenti e votanti.

Letto il presente verbale viene sottoscritto a sensi dell'art. 43 comma 6 del vigente Statuto.

IL PRESIDENTE	IL SEGRETARIO REGGENTE A SCAVALCO
F.TO MARTINI Dott.ssa Morena	F.TO ZANON Dott. Giuseppe

==========

REFERTO DI PUBBLICAZIONE

(ART. 124 d.Lgs. 267/2000)

Segretario Comunale su conforme dichiarazione del messo che copia del presente verbale viene pubblicato il giorno **11/04/2019** all'albo pretorio ove rimarrà esposto per quindici giorni consecutivi.

Lì, **11/04/2019** **IL SEGRETARIO REGGENTE A SCAVALCO**
F.TO ZANON Dott. Giuseppe

==========

☐ Si certifica che la presente deliberazione, è **DIVENUTA ESECUTIVA** il ..... per decorrenza dei termini ai sensi dell'art. 134 del D.Lgs. n. 267/2000.

lì .....

IL SEGRETARIO COMUNALE
.....

==========