COMUNE DI VILLETTE

Provincia del Verbano-Cusio-Ossola

COPIA

DELIBERAZIONE N. 43

X	Soggetta invio ai Capigruppo Consiliari in elenco.
	Trasmessa alla Prefettura di Verbania in data

Verbale di deliberazione della Giunta Comunale

OGGETTO: REGOLAMENTO UE 679/2016. LEGGE 163/2017. ESAME ED APPROVAZIONE REGOLAMENTO SULLA PROTEZIONE DELLE PERSONE FISICHE E SUL TRATTAMENTO DEI DATI PERSONALI E DETERMINAZIONI CONSEGUENTI.

L'anno **DUEMILADICIOTTO**, addì **VENTIDUE** del mese di **MAGGIO** alle ore **18:30** nella sala delle adunanze.

Previa l'osservanza di tutte le formalità prescritte dalla vigente legge, vennero oggi convocati a seduta i componenti la Giunta Comunale.

All'appello risultano:

				Presente	Assente
1 -	ADORNA	Pierangelo	- Sindaco	X	
2 -	RAMONI	Rosanna	- Vice Sindaco		X
3 -	GNUVA	Mario	- Assessore	X	
			Totale	2	1

Assiste all'adunanza l'infrascritto Segretario Comunale Dr. Biglieri Mauro, il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti, il Sig. Adorna Pierangelo – Sindaco assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

IL SINDACO

- Relazione in merito al fatto che il Parlamento Europeo ed il Consiglio in data 27.04.2016 hanno approvato il Regolamento UE 679/2016 (GDPR – General Data Protection Regulation) in materia di protezione delle persone fisiche con particolare riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, Regolamento questo che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione Europea.

- Il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, diventerà definitivamente ed inderogabilmente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, in quanto non richiede alcuna forma di legislazione applicativa o attuativa da parte degli stati membri.

- In questo contesto 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, oltre alle imprese, dovranno tenere presenti in vista della piena applicazione del Regolamento, prevista il 25 maggio 2018.

- Ai sensi dell'art. 13 della Legge n. 163/25.10.2017 il Governo è stato delegato ad adottare, entro sei mesi dalla sua entrata in vigore, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del 27.04.2016 di che trattasi.

- 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, fin da subito, considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di "Riservatezza" entro il termine perentorio del 25.5.2018.

- Appare in conclusione necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questa Unione Montana, commisurata alla sua strutturazione organizzativa ed al suo organigramma, di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE.

- I presupposti e le correlate prescrizioni surriportate si trasfondono nella schema di Regolamento allegato, proposto in testo che si sviluppa in 11 articoli, mutuato dallo schema proposto dall'A.N.C.I. in un accurato documento che contiene istruzioni tecniche, linee guida, note e modulistica, sottolineando che tale Regolamento sostituisce ad ogni effetto tutta la disciplina vigente in seno a questa Unione Montana in materia di riservatezza e tutela dei dati personali sensibili, con adeguamento della relativa documentazione e modulistica.

- In un'ottica di efficacia dell'azione amministrativa, con questo medesimo provvedimento consiliare saranno subito affrontati e definiti taluni rilevanti adempimenti in materia di individuazione della figura titolare e responsabili del trattamento e della correlata protezione dei dati.

LA GIUNTA COMUNALE

- Visto il Regolamento UE 679/2016 (GDPR – General Data Protection Regulation), approvato dal Parlamento Europeo e dal Consiglio in data 27.04.2016, relativo alla protezione delle persone fisiche, con particolare riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, normativa questa che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione Europea;

- Vista la documentazione predisposta dagli uffici comunali, elaborata sul modello della proposta elaborata dall'A.N.C.I.;

- Considerato di dover procedere al recepimento del Regolamento UE 679/2016, approvato dal Parlamento Europeo in data 27.04.2016, relativo alla protezione delle persone fisiche, con particolare riguardo al trattamento dei dati personali, il cui termine inderogabile è la data del 25 maggio 2018;

- Visto il vigente Statuto Comunale;
- Visto il D.Lgs. 18/08/2000 n. 267;
- Visto che è stato acquisito il parere favorevole, per quanto di competenza, in ordine alla regolarità tecnica espresso dal Segretario Comunale, ai sensi dell'art. 49 del D.Lgs. 18/08/2000 n. 267, nonché l'attestazione sulla copertura finanziaria della spesa;
- Ad unanimità di voti espressi per alzata di mano,

DELIBERA

1. Di fondare il presente provvedimento sull'essenziale relazione esposta in narrativa e sui conseguenti presupposti e premesse che motivano i contenuti e le disposizioni della presente deliberazione e della correlata disciplina, al recepimento del Regolamento UE 679/2016 (GDPR – General Data Protection Regulation), approvato dal Parlamento Europeo in data 27.04.2016, relativo alla protezione delle persone fisiche, con particolare riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, normativa questa che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione Europea.
2. Di approvare conseguentemente il regolamento attuativo del "Regolamento U.E. 2016/679", il quale sostituisce ad ogni effetto tutta la regolamentazione vigente in materia in seno al Comune, nel testo sviluppato in n. 11 articoli, che viene allegato al presente provvedimento per costituirne parte integrante e sostanziale, con ad oggetto: "Disciplina di attuazione del Regolamento U.E 2016/679 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali".
3. Di rimarcare che, anche con successivi provvedimenti, adottati dai soggetti competenti di questa Amministrazione, si procederà ad attuare i diversi adempimenti che ne conseguono, secondo la disciplina stabilita nella presente deliberazione e nel Regolamento approvato, in conformità a quanto stabilito nel Regolamento UE 2016/679, il quale prevede in particolare, tra le incombenze di maggiore rilevanza:
   - l'individuazione puntuale del soggetto Titolare del Trattamento;
   - la designazione del Responsabile della Protezione Dati (RPD);
   - l'istituzione e la gestione del Registro delle attività di trattamento, del Registro delle categorie di attività di trattamento e del Registro Unico dei trattamenti;
   - la messa in atto di misure tecniche e organizzative adeguate per garantire ed essere in grado di mostrare che i trattamenti dei dati personali vengono effettuati in conformità alla disciplina europea, approfondendo quanto già prefissato nel Regolamento;
   - l'aggiornamento della documentazione attualmente in essere ed in uso nell'Ente in relazione al trattamento dei dati personali;
4. Di stabilire sin d'ora e con questo medesimo provvedimento, in conseguenza all'organigramma dell'ente, alla sua strutturazione, alle previsioni statutarie ed alle dimensioni demografiche dell'Ente nonché alla sua incapacità di sostenere a regime la spesa relativa al conferimento a soggetti terzi di incarichi relativi alla presente, che il Sindaco – Legale Rappresentante è il soggetto Titolare del Trattamento dei Dati, l'unico dipendente comunale attualmente in organico è il Responsabile del Trattamento dei dati, mentre il Segretario Comunale viene designato Responsabile della Protezione dei Dati;
5. Con separata votazione unanime espressa per alzata di mano, la presente deliberazione viene dichiarata immediatamente eseguibile ai sensi e per gli effetti dell'art. 134 comma 4° del D. Lgs. n. 267/2000.

****

Letto. confermato e sottoscritto:

Il Presidente — *F.to Adorna Pierangelo*

Il Segretario Comunale — *F.to Dr. Biglieri Mauro*

COMUNICAZIONE AI CAPIGRUPPO CONSILIARI

(Art. 125 D.Lgs. 18/08/2000 n. 267)

Si dà atto che del presente verbale viene data comunicazione oggi 30 maggio 2018, giorno di pubblicazione, ai Capigruppo Consiliari.

Il Segretario Comunale
F.to Dr. Biglieri Mauro

REFERTO DI PUBBLICAZIONE

(Art. 124 del D.Lgs. 18/08/2000 n. 267)

N. 161 Reg. Pubblicazioni

Certifico io sottoscritto Segretario Comunale che copia del presente verbale venne pubblicata in data odierna all'Albo Pretorio Comunale, ove rimarrà esposta per 15 giorni consecutivi.

Villette lì, 30 maggio 2018

Il Segretario Comunale
F.to Dr. Biglieri Mauro

CERTIFICATO DI ESECUTIVITA'

(Art. 134 comma 3° D.Lgs. 18/08/2000 n. 267)

Si certifica che la suestesa deliberazione, non soggetta al controllo preventivo per legittimità, è divenuta esecutiva il 22 maggio 2018:

- ☐ Per decorrenza dei termini, essendo stata pubblicata nelle forme di legge all'Albo Pretorio del Comune, senza riportare, nei primi dieci giorni di pubblicazione, denunce di vizi di legittimità o competenza, ai sensi dell'art. 134 comma 3° del D.Lgs. 18/08/2000 n. 267.
- ☑ Perché dichiarata immediatamente eseguibile, ai sensi dell'art. 134 comma 4° del D.Lgs. 18/08/2000 n. 267.

Il Segretario Comunale

Villette lì, 22 maggio 2018 — F.to Biglieri Dott. Mauro

PARERE DI REGOLARITA' TECNICA

(Art. 149 comma 1° D.Lgs. 18/08/2000 n. 267, come modificato dall'art. 3 del D.L. n. 174/2012)

Il sottoscritto Segretario Comunale esprime parere favorevole sulla proposta della presente deliberazione.

Villette lì, 22 maggio 2018

Il Segretario Comunale
F.to Biglieri Dott. Mauro

Copia conforme all'originale, in carta libera ad uso amministrativo.

Villette lì, 30 maggio 2018

Il Segretario Comunale
Biglieri Dott. Mauro
Firmato in originale agli atti

Comune di Villette

Regione Piemonte
Provincia del Verbano Cusio Ossola

DISCIPLINA di ATTUAZIONE
del REGOLAMENTO UE 679/2016 relativo alla PROTEZIONE delle PERSONE FISICHE
con RIGUARDO al TRATTAMENTO dei DATI PERSONALI

Adottato con deliberazione della Giunta Comunale n. 43 del 22 maggio 2018

Sommario

ART. 1
OGGETTO

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27.04.2016 n. 679), di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, per il Comune di Villette.

ART. 2
TITOLARE DEL TRATTAMENTO

1. Il Comune di Villette, rappresentato ai fini previsti dal RGPD dal Sindaco – Legale Rappresentante, giusta la previsione dello Statuto Comunale vigente, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").

2. Il Titolare e' responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza, limitazione della finalità; minimizzazione dei dati, esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali e' 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 dagli articoli 15-22 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 sono 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, tenuto conto di quanto indicato dal successivo art. 9.

6. Il titolare, inoltre, può all'occorrenza provvedere a:
   a) designare in aggiunta alle figure già preposte (Responsabili delle Posizioni Organizzative delle singole strutture in cui si articola l'organizzazione dell'Unione) eventuali altri Responsabili del trattamento. In tal senso il Titolare può avvalersi anche di soggetti pubblici o privati;
   b) nominare un funzionario che eventualmente collabora con la figura di Responsabile della protezione dei dati;

c) nominare quale Responsabili del trattamento anche i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione, relativamente alle banche dati gestite da soggetti esterni, 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 connesse alle attività istituzionali;

d) predisporre l'elenco dei Responsabili del trattamento derivante dall'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

7. 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
FINALITA' DEL TRATTAMENTO

1. I trattamenti sono compiuti dal Comune per le seguenti finalità:

   a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.
   Rientrano n 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 di statistica;
   - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale, regionale e comunale affidate o attribuite all'Unione Montana in base alla vigente legislazione

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

   b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

   c) l'esecuzione di un contratto con soggetti interessati;

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

ART. 4
RESPONSABILE DEL TRATTAMENTO

1. Il Responsabile del Trattamento è la figura che nell'organigramma del Comune ha diretti compiti gestionali in materia di trattamento dei dati personali nell'ambito del Servizio di cui ha la responsabilità ovvero, se incaricato, del Procedimento di cui ha la responsabilità.

2. Il Responsabile è perciò di norma il Responsabile della specifica "Posizione Organizzativa" che gestisce i dati personali sensibili e le banche dei dati personali esistenti nell'articolazione organizzativa di propria competenza.

   Il Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.

3. Altri dipendenti del Comune, nell'ambito della "Responsabilità di Procedimento", possono essere designati responsabili di specifici trattamenti, mediante incarico del Dirigente, ovvero

del Responsabile di Posizione Organizzativa, con provvedimento (Determinazione, lettera o nota d'incarico, anche convenzione o altro, in relazione allo specifico argomento e funzionalmente commisurato alla sua rilevanza e complessità) nel quale sono in particolare 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;

4. Il Titolare del Trattamento può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie 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.

5. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile di specifici trattamenti devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

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 svolge per conto del Titolare;
   - all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
   - alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
   - 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 e' in possesso;
   - ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

ART. 5
RESPONSABILE DELLA PROTEZIONE DATI

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") e' individuato nella figura unica del Segretario Comunale.

2. Il RPD e in particolare incaricato dei seguenti compiti:
   a) informare e fornire consulenza ai soggetti incaricati 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 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 altre responsabilità che fanno capo nel ruolo di Titolare. 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;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere.

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

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 e' comunicato al Garante;

f) l'eventuale tenuta dei registri di cui ai successivi artt. 7 e 8;

3. Il RPD deve esser tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

   A tal fine:

   - 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 verifiche una violazione dei dati o un altro incidente.

4. 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.

5. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

6. Al RPD sono attribuite le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

   - supporto attivo per lo svolgimento dei compiti da parte dei Responsabili di Posizioni Organizzative e della Giunta dell'Unione, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;
   - tempo sufficiente per l'espletamento di compiti affidati al RPD;

- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione);

7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

   Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Presidente, alla Giunta ed al Consiglio.

   Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso.

ART. 6
SICUREZZA DEL TRATTAMENTO

1. Il Comune di Villette mette in atto le opportune misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio ed anche alle "probabilità e gravità" di 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, a tutela dei diritti e delle libertà delle persone.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:
   - sistemi di autenticazione;
   - sistemi di autorizzazione;
   - sistemi di protezione (antivirus; firewall; antintrusione; altro);
   - misure antincendio;
   - sistemi di rilevazione di intrusione;
   - sistemi di sorveglianza;
   - sistemi di protezione con videosorveglianza;
   - registrazione accessi;
   - porte, armadi e contenitori dotati di serrature e ignifughi;
   - sistemi di copiatura e conservazione di archivi elettronici;
   - altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

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

6. I nominativi ed i dati di contatto del Titolare, dei singoli Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.
7. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D. Lgs. n. 193/6.4.2006).

ART. 7
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto del Comune, del Dirigente, del RPD;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 6.

2. Il Registro è tenuto dal Titolare presso la sede del Comune in forma telematica/cartacea, secondo lo schema *allegato "A"* al presente Regolamento;
   nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.

3. Il Titolare può decidere di tenere un Registro unico dei trattamenti che contiene le informazioni di cui ai comma precedenti e quelle di cui al successivo art. 8, sostituendo entrambe le tipologie di registro dagli stessi disciplinati, secondo lo schema *allegato "C"* al presente Regolamento.
   In tal caso, il Titolare può delegare la sua tenuta ad altro Responsabile unico del trattamento di cui al precedente art. 4.
   Ciascun Responsabile del trattamento ha comunque 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. 8
REGISTRO DELLE CATEGORIE DI ATTIVITA' TRATTATE

1. Il Registro delle categorie di attività trattate da ciascun Responsabile di cui al precedente art. 4, reca le seguenti informazioni:
   a) il nome ed i dati di contatto del Responsabile del trattamento e del RPD;
   b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
   c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 6.

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.

ART. 9
VALUTAZIONI D'IMPATTO SULLA PROTEZIONE DEI DATI

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
   La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tine conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le liberà delle persone fisiche.
   Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) trattamento valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
   b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
   c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
   d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
   e) trattamenti di dati su larga scala, tenendo conto: del numero di numeri di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
   f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
   g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
   h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
   i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

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

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa.

Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Unione.

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

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. 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.

6. La DPIA non e' necessaria nei casi seguenti:
   - se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
   - se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso di possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
   - 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.

   Non e' necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. 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 la gravità dei rischi o, in modo più specifico, di goni 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 die 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.

8. 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.

9. 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.

10. 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. 10
VIOLAZIONE DEI DATI PERSONALI

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distribuzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.

2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy.
   La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.
   Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti.
   - danni fisici, materiali o immateriali alle persone fisiche;
   - perdita del controllo dei dati personali;
   - limitazione dei diritti, discriminazione;
   - furto o usurpazione d'identità;
   - perdite finanziarie, danno economico o sociale;
   - decifratura non autorizzata della pseudonimizzazione;
   - pregiudizio alla reputazione;
   - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.
   I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
   - coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   - riguardare categorie particolari di dati personali;
   - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
   - comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);

- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 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.

7. Tale documentazione deve essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

ART. 11
RINVIO A NORMATIVE

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del **RGPD** e tutte le sue norme attuative vigenti.

****