Approvato con Delibera di Consiglio Comunale n. 44 del 31/07/2018

COMUNE DI TREMESTIERI ETNEO

REGOLAMENTO

Ai sensi dell'art. 30 del Regolamento Europeo 2016/679

General Data Protection Regulation

TITOLARE DEL TRATTAMENTO:	***COMUNE DI TREMESTIERI ETNEO***	**RESPONSABILE PROTEZIONE DATI:**	**Termini Maurizio – CONFORMA S.R.L.S.**
Indirizzo	Piazza Mazzini Tremestieri Etneo	Indirizzo	Via Dante, 127 Ragusa
N. telefono	095 – 7419222	N. telefono	3357699467
Mail	ced@comune.tremestieri.ct.it	Mail	ced@comune.tremestieri.ct.it
Pec.	comune.tremestierietneo@legalmail.it	Pec.	maurizio.termini@ingpec.eu
		Registro tenuto da:	Responsabile protezione dati
		Data	
		Ultimo aggiornamento	
		Prossima revisione	


COMUNE DI TREMESTIERI ETNEO (CT)

SOMMARIO

TITOLO I
Principi Generali

Art. 1
Oggetto e Finalità

1. Il presente Regolamento disciplina le misure organizzative e procedimentali di attuazione del Regolamento UE 2016/679 (R.G.P.D.) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati per finalità istituzionali.
2. Ai fini del presente Regolamento, per funzioni istituzionali si intendono quelle:
   a) previste da leggi o regolamenti statali o regionali, nonché dallo statuto e dai regolamenti comunali;
   b) esercitate in attuazione di convenzioni, accordi/intese nonché sulla base degli strumenti di programmazione e pianificazione previsti dalla legislazione vigente;
   c) svolte in relazione all'esercizio dell'autonomia organizzativa, amministrativa e finanziaria dell'ente locale;
   d) derivanti da esecuzione di contratti e/o accordi con soggetti terzi pubblici e/o privati.

Art. 2
Definizioni

Ai fini del presente regolamento si adottano le seguenti definizioni:

1. **"Dati personali":** qualunque informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2. **"Trattamento":**qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Il Regolamento si applica sia ai trattamenti interamente o parzialmente automatizzati sia a quelli non automatizzati contenuti in un archivio o destinati a figurarvi.
3. **"Limitazione di trattamento"**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4. **"Profilazione":** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5. **"Pseudonimizzazione":**il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6. **"Archivio":**qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7. **"Titolare del trattamento":** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tali trattamenti sono determinati dal diritto dell'Unione Europea o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione

possono essere stabiliti dal diritto dell'Unione o degli Stati membri; ai fini del presente Regolamento si intende il *Comune di Tremestieri Etneo*.

8. **"Responsabile del trattamento":** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9. **"Destinatario":** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazioni di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatarie; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
10. **"Terzo"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
11. **"Consenso dell'interessato":** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano sono oggetto di trattamento con il proprio assenso;
12. **"Violazione dei dati personali"**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
13. **"Dati relativi alla salute":** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute, inclusi i dati genetici e biometrici;
14. **"Dati giudiziari":** i dati personali relativi a condanne penali e ai reati o a connesse misure di sicurezza.
15. **"Autorità di Controllo"**: l'Autorità Pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del Regolamento. In Italia il Garante della Privacy.
16. **"Blocco":** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
17. **"Dato anonimo":** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
18. **"Incaricato del trattamento":** il soggetto o i soggetti che, sotto la diretta autorità del Titolare e del Responsabile (se nominato), e a seguito di loro espressa autorizzazione o ordine di servizio, effettua materialmente le operazioni di trattamento sui dati personali.

Per tutto quanto non espressamente previsto nel presente articolo valgono le definizioni di cui all'articolo 4 R.G.P.D.

Art. 3
Principi applicabili al trattamento dei dati

1. Per le finalità di cui all'art. 1 del presente Regolamento, il Comune effettua il trattamento dei dati personali nel rispetto delle disposizioni del Regolamento UE 2016/679, delle disposizioni nazionali, dei diritti e libertà fondamentali delle persone fisiche, nonché del diritto alla riservatezza ed all'identità delle persone fisiche.
2. I dati personali sono:
   a) trattati in conformità alle norme di legge, cioè in modo lecito, corretto e trasparente;
   b) raccolti per finalità determinate, esplicite e legittime. Le finalità del trattamento devono essere predeterminate e chiare ed eventuali ulteriori trattamenti non devono avere finalità incompatibili con quella originaria. Un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o ai fini statistici non è considerato incompatibile con le finalità iniziali (limitazione della finalità);
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato (limitazione della conservazione);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (integrità e riservatezza).

3. I diritti sui dati personali concernenti persone decedute, possono essere esercitati da chi agisce per la tutela del defunto o per motivi familiari meritevoli di tutela, si applica l'art. 2 terdecies del dlgs. 196 2003 e s.m.i.
4. Il trattamento dei dati osserva il principio di responsabilizzazione che comporta non solo l'obbligo del rispetto delle norme ma anche quello di comprovarlo.

Art. 4
Liceità del trattamento

1. Il trattamento è lecito allorché ricorre almeno una delle seguenti condizioni:
   a) L'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
   b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
   c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
   d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
   e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
   f) Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;
   g) In ogni altro caso previsto dall'art. 9 R.G.D.P.

Art. 5
Trattamenti compatibili

1. Fatti salvi i casi di ulteriori trattamenti effettuati con il consenso degli interessati, per effettuare trattamenti per finalità diverse rispetto a quelle per cui i dati sono stati raccolti, il responsabile del trattamento deve effettuare una valutazione in ottica di bilanciamento degli interessi considerando le seguenti variabili:
   a) presenza di nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
   b) contesto in cui i dati personali sono stati raccolti, in particolare riguardanti la relazione tra l'interessato e il titolare del trattamento;
   c) natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali (ex
   d) dati sensibili) oppure se siano trattati dati relativi a condanne penali e a reati;
   e) possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

f) esistenza di adeguate garanzie che possono comprendere la cifratura o la pseudonimizzazione.

2. Nel caso in cui dalla suddetta valutazione risulti la compatibilità del trattamento, questa si potrà considerare base legittimante il trattamento.

Art. 6
Consenso

1. Il consenso al trattamento dei dati non è richiesto se il Comune agisce nell'ambito delle proprie finalità istituzionali.
2. Il consenso va richiesto se il Comune agisce per specifiche finalità diverse da quelle istituzionali.

In tal caso il Responsabile deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.

3. Il consenso può essere revocato, in tal caso la revoca non pregiudica la liceità del trattamento già effettuato.
4. Alle condizioni per il consenso si applicano gli artt. 7 e 8 del R.G.P.D

Art. 7
Comunicazione e diffusione dati personali

1. La comunicazione fra titolari che effettuano trattamenti di dati personali diversi da quelli ricompresi all'art 9 e all'art. 10 del R.G.P.D, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento; in mancanza di tale norma, la comunicazione è ammessa quando è necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.
2. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste da una norma di legge o, nei casi previsti dalla legge, di regolamento;
3. Si intende per :

a) Comunicazione: il dare conoscenza dei dati personali a uno a più soggetti determinati diversi dall'interessato, dal rappresentante del titolare, dal responsabile, dagli incaricati del trattamento, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
b) Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

TITOLO II
Soggetti del trattamento dei dati

Art.8
Titolare del trattamento

1. Il titolare del trattamento è il soggetto cui competono le decisioni in ordine alle finalità, alle modalità di trattamento di dati personali e strumenti utilizzati.

Il titolare del trattamento dei dati personali ai fini di quanto previsto nel RGPD è il *Comune di Tremestieri Etneo*, rappresentato ai fini legali dal Sindaco pro tempore che si avvale dei Responsabili del trattamento all'uopo nominati.

2. Il *Comune di Tremestieri Etneo* adotta tutte le misure tecniche e organizzative idonee per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali sia conforme ai principi di trattamento del 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, 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;
3. Il titolare del trattamento provvede a nominare i Responsabili del trattamento e il Responsabile della protezione dei dati.
4. Tramite verifiche periodiche il titolare del trattamento vigila sull'osservanza delle indicazioni scritte impartite ai Responsabili e sul pieno rispetto delle vigenti disposizioni e del presente regolamento in materia di trattamento dati.
5. Il Comune è responsabile del rispetto dei principi applicabili al trattamento di dati personali;
6. Il Comune promuove e favorisce l'adesione a codici di condotta elaborati dalle associazioni di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrare il concreto rispetto da parte dei responsabili del trattamento.
7. Nel caso di esercizio associato di funzioni e/o servizi, nonché per i compiti la cui gestione è affidata al Comune da Enti terzi, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità e i mezzi di 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 protezione dei dati personali.

Art. 9
Responsabili del trattamento

1. Il Sindaco del *Comune di Tremestieri Etneo*, nella qualità di titolare del trattamento, nomina, con proprio atto, i responsabili del trattamento, uno per ciascuna struttura di massima dimensione, posizione apicale, fatte salve eventuali diverse misure organizzative;
2. I responsabili del trattamento sono ordinariamente individuati nei funzionari responsabili di struttura, posizione apicale, alta professionalità e sono responsabili per i dati afferenti all'ufficio di appartenenza.
3. Il Comandante della polizia municipale è responsabile anche del trattamento dei dati raccolti sul territorio attraverso la videosorveglianza;
4. Il Sindaco del *Comune di Tremestieri Etneo*, nella qualità di titolare del trattamento, può comunque scegliere di nominare un unico responsabile del Trattamento per tutti i dati afferenti il Comune.
5. Le funzioni dei responsabili del trattamento devono essere specificate nel provvedimento di nomina e devono assicurare, almeno, le seguenti attività:
   a) mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato;
   b) garantire che eventuali incaricati o comunque ogni altro soggetto incaricato, si sia impegnato alla riservatezza, abbia un adeguato obbligo legale alla riservatezza e venga adeguatamente formato;
   c) gestire il registro delle categorie di attività svolte e dei dati trattati;
   d) collaborare alle richieste di accesso, di limitazione ed opposizione degli interessati relativi a trattamenti di dati personali;
   e) effettuare la procedura di valutazione di impatto sulla protezione dei dati (D.P.I.A);
   f) consentire lo svolgimento efficace dei compiti e delle funzioni del Responsabile Protezione Dati;
   g) fornire ogni informazione al Responsabile della protezione dei dati ogni qualvolta debbono essere assunte decisioni che impattano sulla protezione dei dati e consultarlo con immediatezza qualora si verifichi una violazione dei dati o un altro incidente.
   h) trattare i dati seguendo le istruzioni e le normative in materia garantendone la riservatezza.

i) garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione e si sia impegnato alla riservatezza.
j) sensibilizzare e formare il personale che partecipa ai trattamenti ed alle connesse attività di controllo.
k) Informare immediatamente il Responsabile della protezione dei dati, della conoscenza di casi di violazione dei dati personali (c.d. "data breach") di cui all'art.20 per l'eventuale successiva notifica della violazione al Garante della Privacy.

Art. 10
Incaricati del trattamento

1. Ai sensi dell'art. 2 quaterdecies del dlgs. 196/2003 e s.m.i., ogni responsabile del trattamento è, in via generale, autorizzato a nominare incaricati o sub incaricati del trattamento per aree di attività specifica nell'ambito della Direzione/Servizio, con provvedimento formale che:
   a) individua, specifica e delimita l'ambito del trattamento consentito;
   b) contiene specifiche istruzioni ed individua le competenze degli incaricati tra le quali in particolare:
      b1) la comunicazione agli interessati dell'informativa relativa al trattamento dei dati e alla loro diffusione;
      b2) la collaborazione alle richieste di accesso, di limitazione e opposizione degli interessati relative a trattamenti di dati personali effettuati dall'ufficio di propria competenza.

2. La nomina dell'Incaricato, ogni variazione o sostituzione va comunicata al Sindaco e al Responsabile della protezione dei dati.
3. Gli incaricati operano sotto la diretta responsabilità del Responsabile del trattamento che li ha nominati al quale rispondono, fermo restando che la rilevanza esterna per eventuale inadempimento resta in capo al responsabile del trattamento di riferimento, salvo che dimostri che l'inadempimento e/o l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub responsabile.

Art. 11
Responsabili esterni di trattamento

1. Il titolare può avvalersi, per il trattamento di dati, di soggetti pubblici o privati, in qualità di responsabili del trattamento, 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.

Art. 12
Responsabile della protezione dei dati

1. Il titolare del trattamento dei dati nomina con proprio provvedimento il Responsabile della Protezione dei dati (R.P.D.) tra i funzionari responsabili di direzione dell'ente esperti in materia di disciplina della protezione dei dati e della prassi in materia.
2. Il titolare del trattamento garantisce lo svolgimento in modo efficace delle funzioni del Responsabile della protezione dei dati
3. Il R.P.D. può assumere altre competenze interne all'ente che non generino conflitto d'interesse con il suo ruolo principale. Il suo ruolo è incompatibile con quello di Segretario/Direttore Generale e di Responsabile della prevenzione della corruzione.
4. Il titolare del trattamento dei dati, può affidare le funzioni di Responsabile della protezione dei dati anche a soggetti esterni, selezionati con procedura ad evidenza pubblica, tra esperti nella materia. Il Responsabile così selezionato agirà in posizione di autonomia e non avrà ulteriori incarichi nell'ente che possano dare adito a conflitto di interesse. Nel rispetto della normativa vigente in materia, le funzioni, le competenze, i rapporti, sono disciplinati con apposito contratto di servizio il cui contenuto deve essere conforme all'art. 39 del Regolamento UE 2016/679.
5. I Responsabili e gli Incaricati del trattamento devono garantire che il Responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati

personali e supportano e collaborano con il Responsabile della protezione dei dati personali fornendo ogni documento o informazione utile. Il responsabile della protezione dei dati personali riferisce esclusivamente al Sindaco, nella qualità di titolare del trattamento o a un suo delegato.

6. Il responsabile della protezione dei dati è tenuto al segreto sulle attività oggetto delle proprie funzioni.
7. Gli interessati possono rivolgersi al Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei propri dati personali e all'esercizio dei diritti derivanti dal presente regolamento.
8. I dati del R.P.D. e i punti di contatto devono essere pubblicati in via permanente sul sito istituzionale nell'apposita sezione "Amministrazione trasparente" e comunicati al Garante della privacy.

Art. 13
Compiti del Responsabile della protezione dei dati personali

1. Il Responsabile della protezione dei dati personali, nello svolgimento delle proprie funzioni, considera i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. In particolare:
   a) informa e fornisce consulenza al titolare del trattamento e agli incaricati del trattamento e a tutti coloro che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati;
   b) verifica l'applicazione corretta della disciplina sul trattamento dei dati personali e del RGPD , ferma restando la responsabilità degli incaricati del trattamento;
   c) collabora in sede di audit alla mappatura dei processi e all'individuazione delle non conformità per le quali suggerisce misure correttive. Successivamente sovraintende i monitoraggi periodici delle soluzioni adottate per verificare la necessità di eventuali riesami o sostituzione delle misure;
   d) fornisce, se richiesto, il parere sulla necessità di procedere alla valutazione di impatto sulla protezione dei dati personali;
   e) coopera con il Garante e funge da tramite per la consultazione preventiva nel caso in cui residuino rischi elevati in un trattamento, dopo la valutazione di impatto sulla protezione dei dati personali;
   f) fornisce parere al Titolare del trattamento in caso di violazione dei dati personali per la valutazione della gravità del data breach;
   g) supporta le valutazioni di impatto in materia di protezione dei dati;
   h) funge da interfaccia fra i soggetti coinvolti in particolare con l'Autorità di controllo (Garante), gli interessati, le Direzioni e i Servizi dell'Ente;
   i) promuove la cultura della protezione dei dati all'interno dell'ente;
   j) contribuisce a dare attuazione agli elementi essenziali del regolamento quali principi fondamentali del trattamento: i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri del trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.
   k) tiene il Registro unico del Comune di cui al successivo articolo 19.
   l) ha funzioni di monitoraggio, svolge le seguenti funzioni:
      - predispone, in collaborazione con i Responsabili del trattamento, apposito manuale, check list, modulistica e quant'altro necessario per un'omogenea applicazione del Regolamento in tutta l'organizzazione comunale;
      - effettua il primo audit al fine di effettuare una prima ricognizione sullo stato dell'arte e identificare e catalogare tutti gli strumenti di supporto al trattamento dei dati personali per le diverse categorie di dati e tipologie di trattamento;
      - redige l'organigramma dei responsabili del trattamento;
      - effettua nel rispetto dei tempi e modalità del Regolamento i monitoraggi successivi.
   m) si avvale delle segnalazioni e dei controlli effettuati dal responsabile della sicurezza dei sistemi informativi, se nominato;
   n) svolge ogni altra funzione attribuita dal titolare del trattamento che non origini conflitto di interesse.

I responsabili del trattamento hanno l'obbligo di fornire ogni informazione utile ai fini del monitoraggio. I report di monitoraggio vengono trasmessi al titolare del trattamento e possono contenere gli elementi di criticità e le misure di miglioramento.

2. I pareri espressi dal Responsabile Protezione Dati non sono vincolanti per il Titolare del trattamento; tuttavia, l'eventuale adozione di atti o di condotte e/o trattamenti difformi dal parere dev'essere adeguatamente motivata.
3. Il RPD opera in posizione di autonomia nelle svolgimento delle funzioni allo stesso attribuiti.
4. Per lo svolgimento delle proprie funzioni può essere coadiuvato, ove lo ritenga opportuno, da un gruppo di lavoro appositamente costituito.
5. Per l'espletamento delle sue funzioni deve essere garantito al RPD l'accesso a tutte le Direzioni dell'Ente.

TITOLO III
Trattamento dei dati personali

Art. 14
Trattamento di categorie particolari di dati personali (cosiddetti dati sensibili)

1. Gli Uffici del Comune trattano le categorie particolari dei dati personali, di cui all'art. 9 del RGPD, che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, biometrici, relativi alla salute, alla vita sessuale e i dati giudiziari:
   a) per motivi di interesse pubblico rilevante come specificato nel successivo art. 15;
   b) per un interesse vitale dell'interessato o di altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   c) se l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche;
   d) per diritti dell'interessato in materia di diritto del lavoro e sicurezza sociale e protezione sociale autorizzato da norme di legge o contratto collettivo;
   e) se il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
   f) se il trattamento è necessario ai fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici ed è proporzionato alla finalità perseguita.
2. In tutti i casi indicati vanno sempre previste misure di garanzia appropriate e specifiche per tutelare i diritti fondamentali e gli interessati. A tal fine si applicano le misure di sicurezza previste nel Titolo V del presente regolamento.
3. I dati genetici, biometrici e riguardanti lo stato di salute non possono essere diffusi.

Art. 15
Principi di trattamento dei dati particolari e giudiziari

1. I dati particolari di cui all'articolo precedente sono trattati sempre nel rispetto dei principi indicati agli articoli 3 e 4. Devono essere esatti, pertinenti, non eccedenti ed indispensabili rispetto alle finalità perseguite e sono aggiornati periodicamente.
2. I raffronti e le interconnessioni con altre informazioni sensibili e giudiziarie detenute dal Comune sono consentiti soltanto previa verifica della loro stretta indispensabilità nei singoli casi e con l'indicazione scritta dei motivi che ne giustificano l'effettuazione. Lo stesso vale se le predette operazioni sono

effettuate utilizzando banche dati di diversi titolari del trattamento; la diffusione dei dati sensibili e giudiziari, è ammessa esclusivamente previa verifica, nel rispetto dei limiti e con le modalità stabilite dalle disposizioni legislative che le prevedono.

3. Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali sensibili e giudiziari.
4. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica deputata o se autorizzato dal diritto europeo o nazionale che prevede garanzie appropriate per i diritti e la libertà degli interessati.
5. Si applicano i principi disciplinati dall'art. 2 octies del d.lgs. 196/2003 e s.m.i.

Art. 16

Interesse pubblico rilevante

1. I trattamenti di interesse pubblico rilevante effettuati dal *Comune di Tremestieri Etneo* sono:
   a) **Stato civile, Anagrafe e liste elettorali**: sono considerati di rilevante interesse pubblico i trattamenti dei dati relativi alla tenuta degli atti e dei registri dello stato civile, dell'anagrafe sia dei residenti in Italia che degli italiani all'estero, nonché delle liste elettorali e dei diritti elettorali attivi e passivi;
   b) **Cittadinanza, Immigrazione e Condizione dello Straniero:** sono considerati di rilevante interesse pubblico i trattamenti dei dati e le attività dirette all'applicazione della disciplina in materia di cittadinanza, di immigrazione, di asilo, di condizione dello straniero e di profugo e sullo stato di rifugiato. In particolare è ammesso il trattamento dei dati strettamente necessari per l'adozione di atti e provvedimenti quali rilascio di visti, permessi, attestazioni, autorizzazioni, certificati o altri documenti richiesti dei terzi legittimati;
   c) **Esercizio dei diritti politici e pubblicità dell'attività degli organi dell'ente**: sono considerate di rilevante interesse pubblico le attività finalizzate all'applicazione della disciplina in materia di elettorato attivo e passivo e di esercizio di altri diritti politici, nonché dirette all'esercizio del mandato degli organi rappresentativi. Sono altresì rilevanti le attività finalizzate all'applicazione della disciplina relativa alla documentazione dell'attività istituzionale degli organi dell'ente.
   d) **Rapporti di lavoro:** sono considerate di rilevante interesse pubblico le attività finalizzate all'instaurazione ed alla gestione dei rapporti di lavoro sia in ordine agli adempimenti previsti in relazione al trattamento economico e giuridico, sia in materia sindacale, disciplinare, e di igiene e sicurezza del lavoro.
   e) **Materia tributaria**: sono considerate di rilevante interesse pubblico le attività dirette all'applicazione, anche tramite concessionari del servizio, delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti e i responsabili d'imposta , nonché in materia di deduzioni, detrazioni e sgravi.
   f) **Benefici economici**: sono considerate di rilevante interesse pubblico le attività finalizzate all'applicazione della disciplina in materia di benefici economici, agevolazioni, elargizioni e altri emolumenti, certificazione ISEE.
   g) **Autorizzazioni e Abilitazioni**: sono considerate di rilevante interesse pubblico le attività relative alle certificazioni, autorizzazioni, licenze, passi carrai, stalli sosta disabili, carico/scarico merci, sosta temporanea, occupazione suolo pubblico. Tra queste sono comprese le certificazioni e le informazioni previste dalla normativa antimafia e quelle relative alla normativa in materia di usura e antiracket e protocolli di legalità stipulati con la Prefettura e con soggetti terzi, Sportello SUAP.
   h) **Servizi Sociali**: sono considerate di rilevante interesse pubblico le attività di welfare con particolare riferimento a:
      - assistenza nei confronti dei minori, anche in relazione a vicende giudiziarie;
      - interventi di sostegno psico-sociale, economico e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare, ivi compresi dati di minori in carico ai servizi sociali;

- interventi anche di rilievo sanitario in favore di soggetti bisognosi, non autosufficienti o incapaci , ivi compresi i servizi di assistenza economica, domiciliare, di telesoccorso, accompagnamento e trasporto;

i) **Volontariato e Associazionismo**: sono considerate di rilevante interesse pubblico le attività finalizzate all'applicazione della disciplina in materia di rapporti con le organizzazioni di volontariato anche con riferimento al trattamento dei dati di cui alla precedente lettera h, e per le attività svolte in partenariato pubblico-privato sociale;

j) **Attività di predisposizione di elementi di tutela in sede amministrativa o giurisdizionale**: sono di rilevante interesse pubblico le attività finalizzate alla tutela dell'ente in sede amministrativa e giurisdizionale.

k) **Esercizio del diritto d'accesso**: sono di rilevante interesse pubblico i trattamenti di dati in conformità di leggi per l'applicazione della disciplina sull'accesso ai documenti amministrativi e la tenuta del registro degli accessi.

l) **Rapporti con enti di culto**: sono considerati di rilevante interesse pubblico i trattamenti strettamente necessari allo svolgimento di rapporti istituzionali con gli enti di culto, con le confessioni e le comunità religiose.

m) **Altre categorie di dati di rilevante interesse pubblico**: sono considerati di rilevante interesse pubblico i trattamenti di dati connessi all'irrogazione di sanzioni amministrative, dati di visura dei veicoli, dati verifiche partenariato, dati per ricorsi e contenziosi, dati acquisiti tramite impianti di videosorveglianza, dati delle strutture ricettive, dati di soggetti coinvolti in infortuni stradali.

n) **Contratti**: sono considerati di rilevante interesse pubblico i trattamenti di dati connessi alla conclusione e all'esecuzione di contratti pubblici, ivi compresi i dati relativi alle operazioni di pagamento.

o) **Quanto previsto nell'art.** 2 sexies del d.lgs. 196/2003 e s.m.i.

Art. 17
Obblighi di pubblicazione

1. Il Comune di Tremestieri Etneo effettua il trattamento di dati personali, contenuti in atti e documenti amministrativi, che devono essere pubblicati sul web per obblighi di trasparenza previsti da norme di legge.
2. Fermo restando il rispetto della normativa sulla trasparenza e l'accesso, ai fini della pubblicazione non possono essere resi intellegibili i dati non previsti espressamente dalla norma e/o comunque non necessari, eccedenti o non pertinenti con le finalità di pubblicazione.
3. I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacali possono essere diffusi solo se indispensabili; i dati particolari relativi alla vita sessuale non possono essere diffusi.
4. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.
5. I dati personali diversi dai dati sensibili e dai dati giudiziari, possono essere diffusi attraverso siti istituzionali, nonché trattati secondo modalità che ne consentano l'indicizzazione e la rintracciabilità tramite i motori di ricerca web.
6. I dati personali devono essere conservati, in ogni caso, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati; l'interessato ha sempre diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.

Art. 18
Pertinenza delle informazioni contenenti dati personali

1. Non possono essere disposti filtri e altre soluzioni tecniche atte a impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente".
2. Qualora i dati personali contenuti nei documenti non siano pertinenti o siano eccedenti rispetto all'interesse manifestato dal richiedente nell'istanza di ostensione, al fine di salvaguardare la riservatezza

di terzi, l'accesso agli atti può essere limitato, su valutazione del Responsabile del trattamento, mediante l'occultamento di alcuni contenuti.

Art. 19
Trattamento dei dati personali effettuato con sistemi di videosorveglianza

1. La videosorveglianza costituisce un'attività di vigilanza su persone e beni, sostituendo, in tutto o in parte, la presenza umana sul posto,
2. L'attività di videosorveglianza è effettuata:
   - Per finalità di tutela della sicurezza urbana,
   - Salvaguardia del patrimonio comunale e prevenzione vandalismo,
   - Prevenzione del degrado, quali abbandono rifiuti in prossimità di parchi , aree pubbliche, etc.
   - Rispetto della normativa sul traffico e del codice della strada,
   - Corretta osservanza di ordinanze, regolamenti comunali;
3. I sistemi di videosorveglianza non possono essere utilizzati per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati;
4. Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza richiede apposita informativa agli interessati e questa può essere rilasciata in forma semplificata come indicato al successivo art.29;
5. La durata della conservazione dei dati è limitata ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione in conformità dell'art.6, c.9, D.L. N. 11/2009, convertito con Legge 23 aprile 2009, n. 38. Tempi di durata maggiore della conservazione dei dati necessitano di richiesta al Garante adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti;
6. Ai fini di promozione turistica o pubblicitaria possono essere utilizzate web-cam o camera on line, in questo caso non devono essere rese visibili le persone riprese, adottando opportuni angoli di ripresa, o una distanza tale da non permettere il riconoscimento dei tratti somatici, evitando funzioni di zoom e utilizzando una bassa risoluzione della ripresa;
7. Ai fini di maggiore trasparenza e pubblicità le riprese audiovisive delle sedute del consiglio comunale sono disciplinate dall'apposito regolamento di cui alla delibera consiliare n. 133 del 11.12.2013, integrato dal presente;
8. Ai dati raccolti mediante sistemi di videosorveglianza, vanno applicate misure di sicurezza adeguate ai sensi del successivo art. 29;

Art. 20
Registri delle attività di trattamento

1. Il *Comune di Tremestieri Etneo*, nella qualità di titolare del trattamento, istituisce e tiene aggiornato, in forma scritta e/o in formato elettronico, il Registro Unico del trattamento dell'Ente.
2. Il registro unico della Privacy deve contenere almeno le seguenti informazioni:
   a) Estremi identificativi e di contatto del Comune e del titolare del Trattamento;
   b) Estremi identificativi e di contatto dei responsabili del trattamento e degli eventuali incaricati;
   c) Estremi identificativi e di contatto del responsabile della protezione dei dati;
   d) Finalità di trattamento;
   e) Descrizione delle categorie di interessati e delle categorie di dati personali;
   f) Categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   g) Eventuali trasferimenti di dati personali verso un Paese terzo o un'Organizzazione internazionale con documentazione delle garanzie in materia di privacy;
   h) Termini ultimi previsti per la cancellazione delle diverse categorie di dati, ove possibile;
   i) Descrizione generale delle misure di sicurezza tecniche e organizzative adottate;
   j) Il presupposto normativo del trattamento;
   k) Le operazioni eseguite per il trattamento;
   l) Una sintetica descrizione del trattamento e del flusso informativo.

3. Ogni Responsabile del trattamento istituisce e tiene aggiornato, in forma scritta e/o in formato elettronico, un registro delle categorie di attività di trattamento svolte sotto la propria responsabilità.
4. Il registro deve contenere almeno le seguenti informazioni:
   a) Estremi identificativi e di contatto del responsabile del trattamento e degli eventuali incaricati, del titolare del trattamento, del responsabile della protezione dei dati;
   b) Le categorie dei trattamenti effettuati per conto del titolare;
   c) Categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   d) Eventuali trasferimenti di dati personali verso un Paese terzo o un'Organizzazione internazionale con documentazione delle garanzie in materia di privacy;
   e) Termini ultimi previsti per la cancellazione delle diverse categorie di dati, ove possibile;
   f) Descrizione generale delle misure di sicurezza tecniche e organizzative adottate;
   g) Il presupposto normativo del trattamento;
   h) Le operazioni eseguite per il trattamento;
   i) Una sintetica descrizione del trattamento e del flusso informativo.
5. I registri devono essere tenuti costantemente aggiornati.
6. Il registro unico del trattamento viene costruito attraverso il trasferimento delle informazioni contenute nel registro dei Responsabili del trattamento al Responsabile della protezione dei dati, che provvede ad assemblare, previa verifica, dette informazioni e a tenerlo costantemente aggiornato.
7. In caso di richiesta del Garante, il Registro Privacy è messo immediatamente a disposizione.

Art. 21
Violazione dei dati personali (data breach)

Per violazione dei dati personali si intende la violazione di sicurezza (data breach) che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati:
La violazione dovrà essere notificata al Garante della privacy senza ingiustificato ritardo e ove possibile, entro 72 ore dal momento in cui il titolare del trattamento ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche; In caso di violazioni di dati personali si applicano gli artt. 33 e 34 del RGPD.

TITOLO IV
DIRITTI DEGLI INTERESSATI

Art. 22
Diritto di trasparenza

1. Il principio di trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro.
2. L'interessato deve essere messo in condizione di poter ricevere le informazioni relative al trattamento di dati personali che lo riguardano al momento della raccolta del dato o comunque entro un tempo ragionevole nel caso in cui i dati non siano da lui direttamente forniti.
3. Le informazioni che devono essere fornite all'interessato, tramite l'informativa devono contenere almeno i dati di cui ai successivi articoli 28 e 29 del presente Regolamento.

Art. 23
Diritto d'accesso e alla portabilità dei dati

1. L'interessato ha sempre diritto di ottenere dal Responsabile del trattamento la conferma che sia in corso un trattamento dei dati personali che lo riguardano, di averne accesso e di acquisire informazioni circa:
   a) Finalità del trattamento;
   b) Categoria dei dati trattati;

c) I destinatari a cui i dati personali sono o saranno comunicati;
d) Il periodo di conservazione dei dati previsto o, se non è possibile, i criteri utilizzati per determinare tali periodi;
e) L'esistenza del proprio diritto a richiedere la rettifica o cancellazione del dato o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) L'esistenza di un processo decisionale automatizzato, compresa la profilazione dei dati, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. La richiesta va inoltrata in forma scritta dall'interessato senza particolari formalità: in caso sia inoltrata con mezzi elettronici, salvo contraria indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.
3. Nel caso in cui il titolare del trattamento tratti una notevole quantità di dati che riguardano il soggetto interessato, può fare richiesta allo stesso di specificare le informazioni o le attività di trattamento alle quali la richiesta si riferisce.
4. Il Responsabile del trattamento deve fornire risposte entro trenta giorni dal ricevimento della richiesta; tale termine può essere prorogato di ulteriori sessanta giorni in casi di particolare complessità, ma, in tal caso, l'interessato va avvisato del differimento entro trenta giorni dall'istanza.
5. L'incaricato del trattamento e i sub incaricati sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole. In tale ipotesi, va rilasciata copia del documento richiesto.
6. Il rilascio della copia è gratuito; salvo il costo di riproduzione per le copie su carta.
7. Il diritto alla portabilità dei dati di cui all'articolo 20 del R.G.P.D., cioè il diritto di ricevere in formato strutturato i propri dati personali e di trasmettere tali dati ad altro titolare, non si applica ai trattamenti svolti dal Comune necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso ente.

Art. 24
Diritto di limitazione

1. L'interessato, previa richiesta scritta, ha diritto ad ottenere la limitazione del trattamento:
   a) in caso di contestazione sull'esattezza dei dati personali, per il periodo necessario alla verifica da parte del Comune;
   b) in caso di trattamento illecito, se l'interessato si opponga alla cancellazione di dati chiedendo invece che ne sia limitato l'utilizzo;
   c) in caso di esercizio del diritto di opposizione nell'attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
2. Il Responsabile del trattamento deve fornire risposta entro trenta giorni dal ricevimento della richiesta: tale termine può essere prorogato di ulteriori sessanta giorni in caso di particolare complessità, ma, in tal caso, l'interessato va avvisato del differimento entro trenta giorni dall'istanza.
3. L'incaricato del trattamento e i sub incaricati, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, ove necessario, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.
4. In caso di riscontro favorevole va comunicato all'interessato che ha ottenuto la limitazione del trattamento, senza ritardo e prima che la limitazione sia revocata. Vanno altresì avvisati i destinatari della limitazione dei dati, salvo ciò non sia possibile o richieda un motivato sforzo sproporzionato.

Art. 25
Cancellazione e Diritto all'oblio

1. L'interessato può presentare per iscritta istanza per la cancellazione dei dati personali che lo riguardano:
   a) se non sono più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati;

b) se revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;
c) se i dati sono illecitamente trattati;
d) se i dati devono essere cancellati per adempiere ad un obbligo normativo cui è soggetto il titolare del trattamento.

2. Il Responsabile del trattamento deve fornire risposta entro trenta giorni dal ricevimento della richiesta; tale termine può essere prorogato di ulteriori sessanta giorni in casi di particolare complessità ma, in tal caso, l'interessato va avvisato del differimento entro trenta giorni dall'istanza.
3. L'incaricato del trattamento e i sub-incaricati, sono tenuti a collaborare per la verifica della sussistenza del diritto, chiedendo, ove necessario, informazioni all'interessato, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.
4. Nel caso che i dati siano stati diffusi pubblicamente, anche su siti web, l'incaricato del trattamento, tenendo conto dei costi di attuazione, è tenuto a informare gli altri titolari che trattano i medesimi dati, della richiesta di cancellazione degli stessi, salvo che ciò non sia possibile o richieda uno sforzo sproporzionato.
5. Il diritto alla cancellazione dei dati non è esercitabile nel caso in cui l'ulteriore conservazione dei dati personali sia necessaria per esercitare il diritto alla libertà di informazione e di espressione, per adempiere a un obbligo legale, per eseguire una funzione di interesse pubblico o nell'esercizio di pubblici poteri cui è investito il titolare del trattamento, a fini di archiviazione, di ricerca scientifica o storica o a fini statistici, ovvero per accertare o difendere un diritto in sede giudiziaria.

Art. 26
Diritto alla rettifica dei dati

1. L'interessato può presentare per iscritto istanza per la rettifica da parte del Comune dei dati personali inesatti che lo riguardano. Tenendo conto della finalità del trattamento, l'interessato ha diritto di ottenere anche l'integrazione dei dati personali incompleti, fornendo una dichiarazione integrativa.
2. Il Responsabile del trattamento deve fornire risposta entro trenta giorni dal ricevimento della richiesta; tale termine può essere prorogato di ulteriori sessanta giorni in casi di particolare complessità ma, in tal caso, l'interessato va avvisato del differimento entro trenta giorni dall'istanza.
3. L'incaricato del trattamento ed i sub incaricati sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo, ove necessario, informazioni all'interessato anche al fine di identificarlo e, successivamente, per dare seguito all'esercizio del diritto dell'interessato.

Art. 27
Diritto di opposizione

1. L'interessato può presentare per iscritto richiesta di opposizione al trattamento dei dati personali che lo riguardano; l'opposizione può essere esercitata nei seguenti casi:
   a) per motivi connessi alla situazione particolare dell'interessato, con riguardo a quei trattamenti effettuati per scopo di interesse pubblico o legittimo interesse del titolare compresa la profilazione;
   b) trattamenti effettuati per finalità di marketing;
   c) trattamenti effettuati con finalità di ricerca scientifica o storica o a fini statistici ad eccezione dei casi in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico;

2. Il Responsabile del trattamento entro trenta giorni fornisce risposta all'interessato a seguito della valutazione della situazione. L'opposizione è accolta se non esistono comprovati motivi, basati su norma di legge, per procedere al trattamento, prevalenti sugli interessi del richiedente o se si tratta di esercizio o accertamento di un diritto in sede giudiziaria.

3. Il termine di cui al precedente comma può essere prorogato di ulteriori sessanta giorni in casi di particolare complessità ma, in tal caso, l'interessato va avvisato del differimento entro trenta giorni dall'istanza.

4. L'incaricato e i sub incaricati sono tenuti a collaborare nel procedimento interno di verifica dei presupposti del diritto di opposizione.

5. In ogni comunicazione all'interessato deve essere inserito l'avviso, in modo chiaro e separato dal restante contenuto dell'atto, che questi può esercitare il diritto all'opposizione.

Art. 28
Obbligo di informativa

1. Prima che inizi qualunque trattamento di dati personali, il Responsabile del trattamento fornisce all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti.
2. L'informativa sulla privacy deve essere fornita per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richiede espressamente, anche verbalmente, previa verifica dell'identità dell'interessato.

Essa va effettuata:

a) in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, nel momento della raccolta dei dati;
b) in caso di dati personali non ottenuti presso l'interessato i medesimi dati vanno comunicati:
   - entro un termine ragionevole, massimo di un mese dalla raccolta nel caso in cui i dati vadano comunicati all'interessato alla prima comunicazione;
   - se i dati personali devono essere comunicati ad altro destinatario, non oltre la prima comunicazione;

3. Non è necessario fornire l'informativa:
   a) nel caso in cui l'interessato disponga già di tutte le informazioni necessarie;
   b) nel caso in cui la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi il comune adotta misure comunque proporzionate per tutelare i diritti dell'interessato anche con pubbliche informazioni;
   c) in presenza di un obbligo di legge che impone la riservatezza e segretezza dei dati personali.

Art. 29
Forma e contenuto dell'Informativa

1. L'informativa deve essere sintetica, presentare un linguaggio chiaro e semplice ed essere, in ogni caso, comprensibile per l'interessato.
2. Deve presentare il seguente contenuto:
   a) l'indicazione del Comune quale titolare del trattamento, del responsabile del trattamento e del responsabile della protezione dei dati;
   b) l'indicazione di ogni finalità istituzionale di trattamento e della norma giuridica di riferimento;
   c) l'indicazione di finalità aventi fondamento in contratto o in richiesta dell'interessato;
   d) indicazione delle modalità di trattamento distinte anche in base alla Direzione/Servizio/Ufficio del Comune che lo effettua, evidenziando se sia un trattamento automatizzato (con eventuale possibilità di profilazione) o se sia un trattamento cartaceo;
   e) indicazione dei destinatari;
   f) il periodo di conservazione dei dati personali e, se non previsto da norma di legge, il criterio utilizzato per la durata del trattamento;
   g) l'indicazione dei diritti che l'interessato può esercitare, ovvero: accesso, integrazione, rettifica, eventuale revoca, portabilità, oblio, opposizione e reclamo;
   h) le conseguenze in caso di rifiuto del trattamento odi omessa comunicazione dei dati.

3. Il Responsabile del trattamento può di volta in volta aggiungere ogni ulteriore informazione che si ritiene necessaria al caso concreto.

Art. 30
Informativa per utilizzo di sistemi di videosorveglianza

1. Nel caso di utilizzo di sistemi di videosorveglianza, gli interessati devono essere informati che stanno per accedere in una zona video sorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici.

A tal fine può essere utilizzato un modello di informativa semplificata che poi rinvii a un testo contenente tutti gli elementi completi di cui all'articolo precedente, disponibile agevolmente senza oneri per gli interessati, sia nel sito internet dell'Ente, sia affisso nella sede della Polizia Municipale.

2. Il supporto con l'informativa:
   a) deve essere nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
   b) deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
   c) può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati, al fine di informare se le immagini sono solo visionate o anche registrate.

Art. 31
Limitazione dell'esercizio dei diritti dell'interessato

1. Ai sensi della vigente normativa nazionale il diritto degli interessati può subire limitazioni per le seguenti ragioni:
   - la sicurezza nazionale;
   - la difesa;
   - la sicurezza pubblica;
   - la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, inclusa la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
   - altri importanti obiettivi di interesse pubblico generale dell'unione europea o nazionale, in particolare un rilevante interesse economico o finanziario, anche in materia monetaria, di bilancio e tributario, di sanità pubblica e sicurezza sociale;
   - la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
   - le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
   - una funzione di controllo, di ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri;
   - la tutela dell'interessato o dei diritti e delle libertà altrui;
   - l'esecuzione delle azioni civili.

2. Le limitazioni all'esercizio dei diritti dell'interessato possono essere imposte solo dalla legge.

Art. 32
Mezzi di ricorso, responsabilità e sanzioni

Qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione di dati personali siano stati violati, l'interessato può proporre reclamo al Garante o ricorso innanzi all'autorità giudiziaria, ai sensi degli art. 140 bis , 141, 142, 143,144, 152 del dlgs. 196/2003 e s.m.i.

TITOLO V
MISURE DI SICUREZZA

Art. 33
Misure di sicurezza preventive

1. Il *Comune di Tremestieri Etneo* adotta misure idonee a soddisfare la protezione dei dati fin dalla progettazione dei dati, ovvero, mette in atto misure tecniche ed organizzative adeguate sia prima del trattamento, sia nell'atto del trattamento stesso come indicate nel presente titolo.
2. In particolare:
   - Utilizza le tecniche di pseudonimizzazione dei dati personali;
   - Tratta i soli dati necessari per ogni specifica finalità al fine di garantire la massima protezione dei dati attraverso il loro minimo trattamento;
   - Custodisce e controlla i dati personali in modo da ridurre al minimo, mediante l'adozione di misure di sicurezza preventive, i rischi di distruzione, perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità pubbliche di raccolta;
   - Provvede a formare il personale sugli obblighi in materia di protezione dei dati personali in relazione alle specifiche competenze rivestite dai singoli dipendenti e dei rispettivi uffici in cui sono inseriti.

Art. 34
Valutazione d'impatto sulla protezione dei dati (D.P.I.A.)

1. Quando un trattamento, anche a seguito di analisi, presenta rischi elevati per i diritti e le libertà degli interessati, oltre ad applicare le misure preventive di cui all'articolo precedente, si procede alla valutazione di impatto sulla protezione dei dati (D.P.I.A.) per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio.
2. Ai fini della decisione di effettuare o meno la D.P.I.A. si tiene anche conto degli elenchi delle tipologie di trattamenti soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante della Privacy.
3. La D.P.I.A. può riguardare una singola operazione di trattamento o due o più trattamenti simili che presentano rischi elevati analoghi.
3. Ricorrono rischi elevati e quindi risulta obbligatoria la valutazione d'impatto in presenza di:
   a) una valutazione sistematica e globale di aspetti personali relativa a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su tali persone fisiche;
   b) trattamento su larga scala di categorie particolari di dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, relativi alla salute, alla vita sessuale o condanne penali, a reati e misure di sicurezza;
   c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. Il Comune, altresì, redige una valutazione di impatto del rischio se ricorrono due dei seguenti indici forniti dal Garante:
   a) Valutazione o assegnazione di un punteggio inclusivo di profilazione, in particolare, in considerazione di 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) Dati sensibili o di carattere altamente personale;
   c) Trattamento di dati su larga scala;
   d) Creazione di corrispondenza o combinazione di insiemi di dati;
   e) Dati relativi a interessati vulnerabili, considerato lo squilibrio di potere tra gli interessati ed il Comune;

f) Uso innovativo o applicazione di nuova tecnologie ed organizzative quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto;

5. Il Comune, se lo ritiene opportuno, può procedere alla D.P.I.A. in caso ricorra anche uno solo degli indici sopra indicati e può individuare anche altri criteri di riscontro del rischio elevato in base alla specifica circostanza o alle specificità del contesto organizzativo.

Art. 35
Contenuto minimo della D.P.I.A.

1. La D.P.I.A. deve presentare il seguente contenuto minimo:
   a) Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
   b) Una valutazione della necessità e proporzionalità dei trattamenti in relazione alla finalità;
   c) Una valutazione dei rischi per i diritti e le libertà degli interessati;
   d) Le misure previste per affrontare i rischi includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità alle disposizioni di legge e del presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati;
   e) I soggetti responsabili, i tempi e i modi di attuazione delle misure.

2. La D.P.I.A. deve essere effettuata dal Responsabile del trattamento con il supporto del Responsabile della protezione dei dati;
3. Nel caso in cui la D.P.I.A. non riesca a trattare in maniera sufficiente i rischi individuati, per quelli residui va effettuata, per il tramite del Responsabile della protezione dei dati, la consultazione del Garante.
4. La sintesi della D.P.I.A. va menzionata all'interno dei procedimenti amministrativi nei quali si inserisce e va riportata in sintesi nei documenti pertinenti.
5. L'esito della valutazione deve essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati rispetti le disposizioni normative.

Art. 36
Consultazione preventiva del Garante della Privacy

1. Nei casi in cui si è proceduto alla valutazione di impatto sulla protezione dei dati ed emerge che il Comune non riesce a trattare in maniera sufficiente tutti i rischi elevati, poiché ne restano ancora alcuni non attenuabili mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, per questi ultimi , va consultato preventivamente il Garante per la Privacy.
2. In tal caso il Comune, per il tramite del Responsabile della protezione dei dati, invia richiesta di consultazione al Garante comunicando:
   a) I dati dell'Ente Locale, in quanto titolare del trattamento, e i propri dati in quanto punto di contatto e referente per la consultazione;
   b) Le finalità ed i mezzi di trattamento previsti;
   c) Le misure di garanzia previste per proteggere i diritti e le libertà fondamentali degli interessati;
   d) La valutazione di impatto sulla protezione dei dati in versione integrale;
   e) Le misure adottate per la riduzione del rischio;
   f) Ogni altra informazione necessaria.

3. Ove ritenuto necessario, il Garante può richiedere al R.P.D. informazioni aggiuntive a quelle già comunicate e può sospendere i termini di cui al comma 3, in attesa della loro trasmissione.

4. In assenza di parere espresso del Garante entro i termini di cui ai commi precedenti, il Comune può procedere al trattamento dei dati.

Art. 37
Misure di sicurezza minime per trattamenti con strumenti elettronici ed informatici

1. Il Responsabile per la protezione dei dati, in collaborazione con i Responsabili del trattamento, controlla le banche dati organizzate in archivi elettronici e fornisce a tutto il personale che le utilizza, le direttive per garantire che le operazioni informatiche di trattamento siano svolte senza rischi per gli interessati. In particolare devono essere adottate le seguenti misure di sicurezza:
   a) Attribuzione agli incaricati di codici identificativi (parola chiave);
   b) Modifica della parola chiave da parte dell'incaricato al primo utilizzo e successivamente ogni sei mesi;
   c) Disattivazione dei codici identificativi nel caso di perdita della qualità degli stessi o di mancato utilizzo per un periodo superiore a sei mesi;
   d) Protezione degli elaborati contro i rischi di intrusioni, mediante l'utilizzo di appositi programmi;
   e) Verifica dell'efficacia e dell'aggiornamento del software antivirus, almeno con cadenza mensile;
   f) Distruzione dei supporti di memorizzazione nel caso non siano utilizzabili;
   g) Applicazione di tecniche di pseudonimizzazione ai dati personali trattati;
   h) Sistemi antintrusione e di protezione, misure antincendio;
   i) Sistemi di copiatura e conservazione di archivi elettronici, misure idonee a ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico.
2. Sono inoltre impartite con circolari interne le istruzioni agli incaricati per non lasciare incustodito ed accessibile il proprio strumento elettronico durante una sessione di trattamento.

Art. 38
Misure per trattamenti non automatizzati

1. Il Comune, anche con il supporto del RPD, fornisce istruzioni scritte agli Incaricati e sub Incaricati del trattamento anche per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici, in particolare, per il controllo e la custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento degli atti e dei documenti contenenti dati personali.
2. I documenti che contengono dati sensibili e giudiziari, sono controllati fino alla restituzione in modo che non accedano ad essi persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
3. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
4. Le persone ammesse, dopo l'orario di chiusura, sono identificate e registrate e se mancano strumenti elettronici di controllo degli accessi agli archivi, questi vanno preventivamente autorizzati.

Art. 39
Misure per dati raccolti con sistemi di videosorveglianza

1. I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
2. Occorre rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando – quando non indispensabili – immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
3. Devono essere adottate almeno le seguenti specifiche tecniche ed organizzative:
   - in presenza di differenti competenze assegnate ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti incaricati o sub incaricati del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ognuno, unicamente le operazioni di propria competenza;

- laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
- nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele:
- in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza di soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
- qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro il rischio di accesso abusivo.

4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza e va determinato con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione.

Art. 40
Disposizioni finali

Il presente Regolamento entra in vigore il giorno in cui diventa esecutiva la delibera di Consiglio che lo approva;

Il presente regolamento abroga il Regolamento di cui alla delibera consiliare n.131 del 20.12.2005 per il trattamento dei dati sensibili e giudiziari ;

Il presente Regolamento abroga il Regolamento di cui alla delibera consiliare n. 8 del 28.01.2010 per il funzionamento degli impianti di videosorveglianza;

Il presente Regolamento sarà pubblicato sul sito internet dell'Amministrazione comunale nella sezione Amministrazione Trasparente ;

Copia del presente Regolamento sarà trasmessa al Segretario Generale, ai Responsabili del trattamento, agli Incaricati del trattamento, al Responsabile della Protezione dei Dati per l'esatta osservanza.