Città di
TREVIGLIO
PROVINCIA DI BERGAMO

REGOLAMENTO

SULL'UTILIZZO DELLA TECNOLOGIA GPS PER LA LOCALIZZAZIONE DEI VEICOLI E DELLE RICETRASMITTENTI DEGLI OPERATORI DI POLIZIA LOCALE.

adottato con deliberazione del
Consiglio Comunale n.26 del 28.04.2026

Città di TREVIGLIO
PROVINCIA DI BERGAMO

INDICE

Art.1		Definizioni
Art.2		Obiettivo del presente Regolamento
Art.3		Ambito di validità e di applicazione del presente regolamento
Art.4		Identificazione del titolare del trattamento dei dati
Art.5		Obiettivi e finalità del sistema di radiolocalizzazione
Art.6		Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza, proporzionalità e finalità
	6.2	Principio di liceità
	6.3	Principio di necessità
	6.4	Principio di non eccedenza e proporzionalità
	6.5	Principio di finalità
Art.7		Accordo con le rappresentanze sindacali
Art.8		Tipologia di veicoli e di soggetti coinvolti
Art.9		Tipi di trattamenti autorizzati
Art.10		Tipologie di soggetti e di strutture coinvolte nelle operazioni di trattamento dei dati
Art.11		Accesso ai dati da parte del personale di Polizia Locale
Art.12		Accesso ai dati da parte dell'Autorità Giudiziaria
Art.13		Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento
Art.14		Principali report/informazioni che il sistema di radiolocalizzazione dovrà produrre
Art.15		Tempi di conservazione dei dati relativi alla geolocalizzazione
Art.16		Modalità di memorizzazione dei dati
Art.17		Ottemperanza al provvedimento del 27-11-2008 del Garante per la protezione dei dati personali relativi al controllo dell'operato degli amministratori di sistema
Art.18		Requisisti minimi sugli strumenti elettronici, informatici e telematici
Art.19		Cessazione del trattamento
Art.20		Limiti alla utilizzabilità dei dati personali
Art.21		Danni cagionati per effetto del trattamento dei dati personali
Art.22		Comunicazione
Art.23		Informativa ai dipendenti
Art.24		Tutela amministrativa e giurisdizionale

Art. 1 – Definizioni.

Ai fini del presente regolamento, si riportano le definizioni inerenti all'attività posta in essere; per le ulteriori definizioni, si rimanda all'art. 4 del DGPR 679/2016 e al D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali, per brevità nel seguito chiamato anche semplicemente "Codice"), come modificato dal D. lgs. 101 del 10.08.2018.

Ai sensi del 1° comma dell'art. 4 del GDPR (Reg. UE 2016/679 si intende per:

A. "trattamento" qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

B. "dato personale" qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

C. "dati identificativi" i dati personali che permettono l'identificazione diretta dell'interessato;

D. "dati particolari" i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

E. "dati giudiziari" i dati personali idonei a rivelare provvedimenti di cui all'articolo 3 comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

F. "titolare" la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

G. "responsabile del trattamento" la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personale;

H. "incaricati" le persone fisiche autorizzate a compiere operazioni di trattamento;

I. "interessato" la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

J. "comunicazione" il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile, dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

K. "diffusione" il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

L. "dato minimo" il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

M. "blocco" la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

N. "banca di dati" qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

O. "Garante" l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

Si intende, inoltre, per:

1) "misure minime" il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 32;

2) "strumenti elettronici" gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

3) "autenticazione informatica" l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

4) "credenziali di autenticazione" i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

5) "parola chiave" componente di una credenziale di una autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

6) "profilo autorizzazione" l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

7) "sistema autorizzazione" l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;

All'interno del presente documento si definisce inoltre:

A) "rischi" situazioni o comportamenti che possono generare un pericolo per i dati personali e/o sensibili. Per meglio valutare l'entità e le azioni da intraprendere il rischio prevede diversi livelli di soglia: basso, medio, grave o gravissimo.
B) "Designato privacy" ai sensi Art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati) del D.Lgs. 196/2003 s.m.i. il titolare può prevedere sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la propria autorità. Il Titolare istituisce la figura del "Designato privacy" e lo individua nel Dirigente del settore Polizia Locale. Il Titolare con

apposita nomina definisce che al "Designato privacy" competono le decisioni in ordine alle modalità del trattamento e ai livelli di accesso alle informazioni.

Art. 2 – Obiettivo del presente Regolamento.

Obiettivo del presente regolamento è normare l'utilizzo di apparati e tecnologie GPS (Global Positioning System) per effettuare la localizzazione dei veicoli e del personale appartenente al Servizio Unificato di Polizia Locale.
Detti dispositivi, pertanto, non saranno utilizzati come strumenti per seguire o monitorare il comportamento o gli spostamenti degli agenti in servizio o di altro personale, ai fini della verifica del puntuale esercizio dell'attività lavorativa.
Il presente regolamento assicura che i trattamenti dei dati personali effettuati dal Settore Sicurezza mediante il sistema di radiolocalizzazione GPS avvengano correttamente, lecitamente, e conformemente a quanto disposto dal Garante per la protezione dei dati personali e, in generale, in conformità alle prescrizioni del GDPR 679/2016 e del D. lgs. 196/2003, come novellato dal D. lgs. 101 del 10.08.2018, e successive modificazioni, oltre a quanto indicato nei vari provvedimenti del Garante per la protezione dei dati personali ed ai principi di liceità, necessità, non eccedenza e proporzionalità e finalità.

Art. 3 – Ambito di validità e di applicazione del presente regolamento.

Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali effettuati mediante utilizzo di apparati e tecnologie GPS per la radiolocalizzazione dei veicoli e delle ricetrasmittenti assegnate in dotazione al personale di Polizia Locale, per l'espletamento dei servizi esterni.

Art. 4 – Identificazione del titolare e del responsabile interno del trattamento dei dati.

Il titolare dei trattamenti di dati personali effettuati mediante il sistema di radiolocalizzazione GPS è il Comune di Treviglio, rappresentato dal Sindaco pro tempore, mentre il designato privacy è il Dirigente del settore Polizia Locale, al quale competono le decisioni in ordine alle finalità e alle modalità del trattamento, compreso anche il profilo della sicurezza.
A titolo esemplificativo e non esaustivo, si riportano di seguito alcuni provvedimenti che spettano esclusivamente al Responsabile del Settore Sicurezza e a chi ne fa le veci:

- Individuazione del numero e tipologia di apparati di radiolocalizzazione GPS da installare;
- Individuazione dei tempi massimi e minimi di conservazione dei dati relativi alla geolocalizzazione;
- Individuazione degli strumenti elettronici, informatici e telematici da utilizzare per la gestione dei dati relativi alla geolocalizzazione, compresa la memorizzazione dei dati stessi;
- l'individuazione dei soggetti che possono essere a vario titolo coinvolti (in qualità di incaricati) nelle operazioni di trattamento dei dati e nelle operazioni di amministrazione di gestione di sistema informatico e telematico;
- Assegnazione di compiti e responsabilità ai soggetti individuati in precedenza.

Art. 5 – Obiettivi e finalità del sistema di radiolocalizzazione.

Il sistema di radiolocalizzazione GPS, in quanto sistema che comporta il trattamento dei dati personali, può essere utilizzato (ai sensi del'art. 6 comma 1 lettera e) del GDPR 679/2016 esclusivamente per il perseguimento delle funzioni istituzionali del servizio di Polizia Locale.
Le finalità per le quali gli apparati e le tecnologie di radiolocalizzazione GPS possono essere lecitamente utilizzati dal Servizio di Polizia Locale sono le seguenti:

- assicurare la sicurezza e l'incolumità del personale di Polizia Locale impegnato sul territorio;
- fornire un ausilio per ottimizzare l'utilizzo operativo del personale e dei veicoli utilizzati dalla Polizia Locale;
- fornire un ausilio per rilevazioni di tipo quantitativo e statistico;
- per ragioni di giustizia, su richiesta dell'Autorità Giudiziaria.

Art. 6 – Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza e proporzionalità e finalità.

6.1. Premessa
La verifica del rispetto dei principi di liceità, necessità, non eccedenza e proporzionalità e finalità dovrà venire effettuata periodicamente sia nei confronti del sistema da radiolocalizzazione nel suo complesso, sia nei confronti di ciascun apparato installato.

6.2 Principio di liceità
Affinché sia soddisfatto il principio di liceità, si dovrà periodicamente verificare che:
- le finalità perseguite mediante il sistema di radiolocalizzazione siano coerenti e compatibili con le funzioni istituzionali di competenza del servizio di Polizia Locale;
- l'utilizzo di apparati e tecnologie GPS non avvenga in violazione delle tutele riconosciute ai lavoratori, con particolare riferimento a quanto previsto dalla legge 300/1970 (Statuto dei Lavoratori).

6.3 Principio di necessità
Affinché sia rispettato il principio di necessità deve essere escluso qualsiasi utilizzo superfluo ed evitati eccessi e ridondanze. Inoltre, il sistema informatico e ciascun apparato GPS deve essere configurato ed utilizzato in maniera tale da non utilizzare dati relativi a soggetti identificabili quando le finalità del trattamento possono essere perseguite raccogliendo solamente dati anonimi;
Inoltre il software deve essere configurato in modo da cancellare automaticamente e periodicamente i dati eventualmente registrati, rispettando il limite massimo di conservazione di 90 giorni.

Ulteriori considerazioni da tenere presenti per il rispetto del principio di necessità sono le seguenti:

- l'esigenza di perseguire le finalità deve essere concreta, reale e comprovabile;
- il sistema di radiolocalizzazione GPS deve essere configurato per l'utilizzazione al minimo di dati personali e di dati identificativi in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od

opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

6.4 Principio di non eccedenza e proporzionalità
Il rispetto dei principi di non eccedenza e proporzionalità si dovrà valutare periodicamente con riferimento ai criteri di seguito elencati:

- il numero e la collocazione degli apparati GPS devono essere effettivamente commisurati al reale livello di necessità, evitando la rilevazione o la registrazione nei casi in cui la radiolocalizzazione non risulti essere indispensabile;
- il segnale GPS trasmetterà la posizione delle radio veicolari e ricetrasmittenti ogni 30 provvedendo a "refresh" automatico ogni 2 (due) minuti per quanto riguarda le prime ed ogni 5 (cinque) minuti per le seconde;
- gli apparati GPS devono essere collocati, e più in generale la radiolocalizzazione deve essere adottata, solo quando altre misure meno invasive siano state ponderatamente valutate insufficienti o inattuabili, salvaguardando quanto previsto all'art. 2, comma 1, del presente Regolamento;
- se l'installazione degli apparati GPS è finalizzata alla sicurezza del personale e per l'ottimizzazione dell'impiego delle risorse umane, devono risultare insufficienti o inefficaci altre tecniche, quali ad esempio l'impiego di radiotelefoni, telefoni cellulari o utilizzo di telecamere di videosorveglianza;
- la non eccedenza e proporzionalità deve essere valutata, anche periodicamente, in ogni fase e modalità del trattamento; ad esempio, in fase di definizione e assegnazione dei profili di accesso ai dati, i profili dovranno essere configurati e assegnati in maniera che gli incaricati accedano alla minima quantità di dati necessaria per lo svolgimento dei compiti assegnati; come minimo si dovrà prevedere una fondamentale distinzione tra il profilo di tipo "Utente Base" e un profilo più elevato di tipo "Amministratore".

6.5 Principio di finalità
Gli scopi perseguiti devono essere determinati, espliciti e legittimi, ai sensi del Capo II del GDPR 679/2016; sono pertanto esclusi utilizzi indeterminati, occulti e non legittimi. In particolare il titolare o il responsabile potranno perseguire solo finalità di loro pertinenza.

Potranno essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate informative al personale rese ai sensi di quanto previsto (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria) dal Capo III, sezioni I e II GDPR. Non sono ammesse finalità gerarchiche o indeterminate, soprattutto quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti.

È inoltre consentita la radiolocalizzazione come misura complementare volta a supportare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi.

Art. 7 – Accordo con le rappresentanze sindacali.

L'installazione degli apparati muniti della tecnologia GPS deve avvenire previo accordo stipulato con le rappresentanze sindacali. In mancanza di accordo, gli

strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro.

Art. 8 – Tipologia di apparati e di soggetti coinvolti.

Gli apparati GPS potranno essere installati su tutti i veicoli utilizzati dalla Polizia Locale ed anche sugli apparati ricetrasmittenti e/o mobili in dotazione al personale.

Art. 9 – Tipi di trattamenti autorizzati.

Nell'installazione e nell'esercizio del sistema di radiolocalizzazione, sono autorizzati, nei limiti previsti dalla normativa vigente in materia diprotezione dei dati personali, esclusivamente le seguenti tipologie di trattamenti:

- installazione e attivazione di apparati GPS;
- creazione e gestione di gruppi e profili di utenti;
- memorizzazione di dati relativi alla radiolocalizzazione, nel rispetto dei limiti indicati negli artt. 6.3 e 6.4 del presente Regolamento;
- consultazione di dati relativi alla radiolocalizzazione, secondo la ripartizione delle competenze all'interno del settore;
- cancellazione in modo automatico (senza intervento manuale) dei dati relativi alla radiolocalizzazione, nei termini disposti dall'art. 6.3 del presente Regolamento;
- produzione di report;
- localizzazione in tempo reale su mappe di dati relativi alla georeferenziazione;
- installazione e configurazione di software applicativo;
- attivazione collegamenti da remoto solo ed esclusivamente su PC dedicato (in caso di assistenza);
- interventi generici di manutenzione e configurazione hardware e software;
- attivazione e configurazione di meccanismi di logging (tracciatura);
- estrazione e apposizione di forma digitale qualificata a files di log;
- conservazione per almeno tre mesi in luogo sicuro di files di log.

Art. 10 – Tipologie di soggetti e di strutture coinvolte nelle operazioni di trattamento dei dati.

Le operazioni di trattamento dei dati saranno svolte, a vario titolo, dalle seguenti tipologie di soggetti quale espressione del Titolare:

- Designato privacy – Dirigente del settore Polizia Locale, con ruolo di amministratore del sistema e di gestore delle informazioni contenute;
- Altro personale di Polizia Locale, opportunamente designato ed addestrato, munito di credenziali ad uso personale, le cui possibilità di azione all'interno del sistema saranno graduate in relazione al ruolo ricoperto all'interno del Settore, come indicato all'art. 11;
- Personale incaricato della manutenzione degli strumenti elettronici, opportunamente designato tra l'organico dell'ente e all'uopo addestrato;
- Responsabili esterni al trattamento dei dati debitamente nominati;
- Altre pubbliche amministrazioni che richiedano di accedere ai dati per lo svolgimento delle loro funzioni istituzionali: in questo caso l'accesso e l'utilizzo dei dati messi a disposizione dal Comune di Treviglio, avrà luogo sotto la diretta responsabilità e titolarità della pubblica amministrazione o del soggetto richiedente verificare che l'accesso avvenga esclusivamente per lo svolgimento

delle funzioni istituzionali, e non per il perseguimento di interessi o finalità personali o comunque non chiaramente riconducibili allo svolgimento di funzioni istituzionali o di compiti d'ufficio, senza che vi sia abuso d'ufficio. Sarà inoltre cura della Pubblica Amministrazione o del soggetto richiedente o del soggetto al quale i dati sono comunicati o portati a conoscenza a seguito di motivata richiesta, mettere in atto quanto previsto dalla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento all'obbligo di designazione degli incaricati del trattamento, specificando puntualmente per iscritto l'ambito del trattamento consentito e assicurando che le operazioni di trattamento (compresa la mera consultazione, che è comunque una tipologia di trattamento) e l'accesso ai dati avvenga in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Art. 11 – Accesso ai dati da parte del personale di Polizia Locale.

Il personale di Polizia Locale, diverso dal Dirigente del settore, opportunamente designato potrà accedere in tempo reale ai dati per perseguire finalità di sicurezza del personale e per l'ottimizzazione dell'impiego operativo delle risorse umane.
Il Responsabile del Settore ed i soggetti da lui incaricati potranno accedere ai dati per le finalità succitate e inoltre ai fini di rilevazioni statistiche e per ragioni di giustizia.

Verranno predisposti almeno tre diversi livelli di accesso alle informazioni:

- Utente Amministratore individuato nel Responsabile del Settore Sicurezza, ed in sua assenza nel Vicecomandante qualora nominato: questo utente avrà il più ampio accesso possibile a tutte le informazioni detenute dall'impianto, anche con possibilità di modifica delle impostazioni di sistema e la creazione di report;

- Utente Intermedio: assegnato ai soggetti con incarico di particolari responsabilità o con compiti di coordinamento e controllo (es. Ufficiali e titolari di specifiche Responsabilità).
  Questi utenti avranno accesso alle funzioni utili per la gestione delle flotte in tempo reale senza accesso alcuno al materiale conservato in archivio;

- Utente Base: assegnato agli operatori addetti alla Centrale Operativa, con mere funzioni di visualizzazione dei dati, ricezione ed invio di comunicazioni radio e telefoniche. Questo utente sarà abilitato a quanto necessario per supportare l'attività esterna degli operatori, senza alcuna possibilità di modifica delle interfacce o di intervento e visualizzazione delle informazioni registrate, né della reportistica prodotta.

Art. 12 – Accesso ai dati da parte dell'Autorità Giudiziaria.

La comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico può avvenire se prevista da norma di legge o di regolamento, oppure, anche in assenza di norma di legge o di regolamento, se necessaria per lo svolgimento delle funzioni istituzionali.
Pertanto l'Autorità Giudiziaria può, qualora siano in corso indagini, lecitamente richiedere di:

- accedere ai percorsi georeferenziati;
- accedere ai dati relativi alla radiolocalizzazione ed ottenere copia delle registrazioni;

- effettuare registrazioni "ad hoc".

La mancata o tardiva concessione dell'accesso potrà comportare, a carico del soggetto responsabile, il reato di omissione di atti d'ufficio e di ostacolo alle indagini.
Le richieste di accesso/estrazioni dovranno seguire le procedure definite per l'accesso agli atti, ed essere autorizzate dal titolare del trattamento o dal responsabile del trattamento.

In ogni caso, l'utilizzo dei dati da parte di qualsiasi soggetto pubblico, che per l'esercizio delle
proprie funzioni istituzionali abbia necessità di accedere ai dati, dovrà avvenire conformemente a quanto previsto dalla disciplina vigente in materia di privacy e sicurezza.

Art. 13 – Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento.

In generale i soggetti coinvolti nelle operazioni di trattamento dovranno essere designati per iscritto per conto del titolare, dal responsabile interno del trattamento, o dal responsabile del trattamento dei dati, con atto che specifichi chiaramente compiti e responsabilità assegnate. Per quanto riguarda gli incaricati del trattamento dei dati, oltre ai compiti e alle responsabilità affidate, dovrà essere chiaramente specificato l'ambito del trattamento consentito. La revisione della sussistenza delle condizioni per il mantenimento dell'ambito del trattamento consentito del profilo di accesso dovranno essere oggetto di revisione da parte del responsabile o del titolare con frequenza almeno annuale.

Art. 14 – Principali report/informazioni del sistema di radiolocalizzazione.

l sistema di radiolocalizzazione dovrà produrre le seguenti tipologie di report/informazioni:

- posizione istantanea di mezzi ed agenti, per ottimizzare l'impiego del personale in tempo reale;
- estrazione dei percorsi del personale su base oraria o per periodi di tempo limitati nella giornata, eventualmente in forma anonima;
- Chilometri percorsi e tempi di percorrenza.

Art. 15 – Tempi di conservazione dei dati relativi alla geolocalizzazione.

In considerazione delle finalità individuate in precedenza e della necessità di ottemperare al principio di non eccedenza e proporzionalità in tutte le operazioni di trattamento dei dati, i dati relativi alla radiolocalizzazione dovranno essere conservati per un periodo massimo di 90 (novanta) giorni.
È comunque esplicitamente previsto che i tempi di conservazione dei dati relativi alla radiolocalizzazione possano essere ridotti a seguito di variazioni nelle finalità, di mutate esigenze, oppure di motivata richiesta proveniente da altri soggetti pubblici.

Art. 16 – Modalità di memorizzazione dei dati.

Fermo restando i requisiti minimi di sicurezza attuali alla tecnologia disponibile, i dati relativi alla radiolocalizzazione dovranno essere memorizzati in formato elettronico su uno o più supporti di memorizzazione di massa all'interno di un unico e ben determinato apparato di tipo "server" ovvero mediante modalità "cloud".
La memorizzazione temporanea dei dati in locale potrà avvenire solo in caso di estrazione dei dati, nel qual caso la copia temporanea locale dei dati estratti dovrà essere protetta da password e/o criptata.

Art. 17 – Ottemperanza al Provvedimento del 27.11.2008 del Garante per la protezione dei dati personali relativo al controllo dell'operato degli amministratori di sistema.

Per garantire l'ottemperanza a quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 27.11.2008 relativo al controllo dell'operato degli amministratori di sistema, il presente regolamento prevede quanto segue:

- il software della centrale operativa prevede un meccanismo di logging (tracciatura) delle operazioni di amministrazione e gestione di sistema effettuate con profilo di administrator;
- a livello di software di centrale operativa, il suddetto file di log non deve essere sovrascritto per un periodo minimo di 6 mesi;
- il suddetto file di log non dovrà essere per nessun motivo cancellato, modificato o alterato.

Art. 18 – Requisiti minimi sugli strumenti elettronici, informatici e telematici.

Gli strumenti elettronici, informatici e telematici utilizzati nelle operazioni di trattamento dei dati, dovranno soddisfare i seguenti requisiti minimi:

- sistema operativo server e client non obsoleto e con supporto attivo da parte del fornitore;
- server e client protetti da password iniziale di accesso al sistema operativo e alle risorse di rete;
- possibilità da parte dell'utente finale di modificare autonomamente la propria password;
- possibilità da parte dell'amministratore di sistema di disabilitare la user-id senza cancellarla;
- presenza di almeno due profili distinti: uno di tipo "Amministratore" e uno di tipo "Utente Base" a livello di sistema operativo e di tre livelli, "Utente Amministratore" – "Utente Intermedio" – "Utente Base", per il programma applicativo;
- assegnazione e utilizzo delle user-id su base strettamente personale e non di gruppo;
- possibilità di individuare e rimuovere periodicamente le vulnerabilità e le configurazioni poco sicure a livello applicativo e di sistema operativo;
- certificazioni di conformità rilasciate regolarmente da fornitori e installatori, sia in occasione della prima installazione e configurazione, sia in occasione di qualsiasi intervento successivo;
- protezione adeguata da virus e codici maligni;

- protezione perimetrale adeguata in caso di apertura, anche temporanea, ad internet.

I requisiti di cui sopra dovranno essere verificati periodicamente mediante verifiche in loco dei locali, degli apparati e dei programmi, effettuando un'analisi dei rischi e individuando le azioni correttive da mettere in atto.
Periodicamente si dovrà inoltre verificare che le misure pianificate siano state messe in atto e il livello di efficacia delle misure stesse.

Art. 19 – Cessazione del trattamento.

In caso di cessazione del trattamento, i dati dovranno essere distrutti, ad eccezione di quelli per i quali siano in corso o vi siano state in passato richieste di estrazione, che dovranno essere conservati a cura del titolare per fini di documentazione e riscontro.

Art. 20 – Limiti alla utilizzabilità dei dati personali.

La materia è disciplinata dal Capo III, sezione V del GDPR 679/2016.

Art. 21 – Danni cagionati per effetto del trattamento dei dati personali

La materia è disciplinata dall'art. 82 del GDPR 679/2016.

Art. 22 – Comunicazione.

La comunicazione di dati personali da parte del titolare ad altri soggetti pubblici è ammessa quando è prevista da norma di legge o di regolamento attuativo di norma di legge, oppure quando risulti comunque necessaria per lo svolgimento delle funzioni istituzionali.
La comunicazione di dati personali da parte del titolare a privati o ad altri enti pubblici economici è ammessa unicamente quando prevista da norma di legge o di regolamento.

Art. 23 – Informativa ai dipendenti.

Il Titolare del trattamento dei dati dovrà fornire agli interessati un'informativa comprensiva di tutti gli elementi contenuti nell'art 13 del GDPR 679/2016 (tipologia di dati, finalità e modalità del trattamento, compresi i tempi di conservazione), anche in conformità al principio di correttezza in base al quale il titolare è tenuto a rendere chiaramente riconoscibili agli interessati i trattamenti che intende effettuare.

Art. 24 – Tutela amministrativa e giurisdizionale.

Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dall'art. 79 del GDPR 679/2016 e dal D.lgs. 196/2003 s.m.i.