REGIONE LOMBARDIA

CORPO INTERCOMUNALE DI POLIZIA LOCALE
"MARTESANA EST"
COMUNI DI POZZO D'ADDA – TREZZANO ROSA – VAPRIO D'ADDA
Provincia di Milano
20069 – P.zza Cavour, 26 – Tel. 029094428 – Fax. 0290989520 –
E-Mail: polizialocale@comune.vapriodadda.mi.it

Regolamento sull'utilizzo del sistema di gestione delle chiamate tramite centralino telefonico in uso presso il Corpo intercomunale di Polizia Locale

Titolo documento:	**Regolamento sull'utilizzo del sistema di gestione delle chiamate tramite centralino telefonico in uso presso il Corpo intercomunale di Polizia Locale**
Codice documento:	Vaprio – REGTEL-1-0
Nome file:	Vaprio – REGTEL Ver 1-0
Stato documento:	Bozza per revisione e condivisione
Versione:	1.0
Data creazione:	1 ottobre 2014
Data ultimo aggiornamento	10 novembre 2014

Indice

Art. 1 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali, per brevità nel seguito chiamato anche semplicemente "*Codice*").

Ai sensi del 1° comma dell'art. 4 del Codice 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 sensibili*"	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"*	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
h) *"incaricati"*	le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
i) *"interessato"*	la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
l) *"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 e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
m) *"diffusione"*	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
n) *"dato anonimo"*	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
o) *"blocco"*	la conservazione di dati personali con sospensione temporanea di

	ogni altra operazione del trattamento;
p) *"banca di dati"*	qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
q) *"Garante"*	l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

Ai sensi del 3° comma dell'art. 4 del Codice si intende, inoltre, per:

a) *"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 31;
b) *"strumenti elettronici"*	gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
c)*"autenticazione informatica"*	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
d) *"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;
e) *"parola chiave"*	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
f) *"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;
g) *"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:

h) *"rischi"*	Situazioni o comportamenti che possano 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;

Art. 2 - Obiettivo del presente Regolamento

Obiettivo del presente regolamento è normare l'utilizzo del sistema di gestione delle chiamate tramite centralino telefonico in uso presso il Corpo Intercomunale di Polizia Locale tra i Comuni di Pozzo d'Adda, Trezzano Rosa e Vaprio d'Adda.

In particolare, il presente regolamento assicura che i trattamenti di dati personali e sensibili effettuati dal Corpo Intercomunale "Martesana Est" mediante il sistema di gestione delle chiamate tramite centralino telefonico avvengano correttamente, lecitamente, e conformemente a quanto previsto dalla disciplina rilevante in materia di sicurezza e protezione dei dati personali; in particolare, il rispetto del presente regolamento garantirà la conformità:

- alle prescrizioni del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali) e dei vari Provvedimenti del Garante per la protezione dei dati personali;
- al Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003);
- ai provvedimenti del Garante per la protezione del dati personali;
- ai principi di:
    - liceità;
    - necessità;
    - non eccedenza e proporzionalità;
    - 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 e sensibili effettuati mediante il sistema di gestione delle chiamate tramite centralino telefonico in uso presso il Corpo di Polizia Locale "Martesana Est":

- sotto la **diretta titolarità** del Corpo Intercomunale "Martesana Est, e
- sia per le chiamate in entrata che per le chiamate in uscita.

Art. 4 - Identificazione del titolare del trattamento dei dati

Il titolare dei trattamenti di dati personali effettuati mediante il sistema di gestione delle chiamate è il Corpo Intercomunale "Martesana Est" (nel seguito per brevità denominato semplicemente "Corpo Intercomunale"): pertanto, competono esclusivamente al Corpo Intercomunale 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 alcune decisioni che spettano esclusivamente al Corpo Intercomunale:

- il luogo di installazione del centralino telefonico;
- il luogo di conservazione dei dati relativi alle chiamate;
- i tempi massimi e minimi di conservazione dei dati relativi alle chiamate;
- gli strumenti elettronici, informatici e telematici da utilizzare per la gestione dei dati relativi alle chiamate, compresa la memorizzazione dei dati stessi;
- l'individuazione dei soggetti che possono essere a vario titolo coinvolti (in qualità di incaricati, oppure di responsabili interni od esterni oppure di autonomi titolari) nelle operazioni di trattamento dai dati e nelle operazioni di amministrazione di gestione di sistema informatico e telematico;
- l'individuazione di compiti e responsabilità da assegnare ai soggetti individuati in precedenza.

Art. 5 - Obiettivi e finalità del sistema di gestione delle chiamate

Il sistema di gestione delle chiamate, in quanto sistema che comporta il trattamento di dati personali, può venire utilizzato (ai sensi dell'art. 18 comma 2 del D.Lgs. 196/2003) esclusivamente per il perseguimento delle funzioni istituzionali del titolare del trattamento dei dati, vale a dire del Corpo Intercomunale.

Le finalità per le quali il sistema di gestione delle chiamate può essere lecitamente utilizzato dal Corpo Intercomunale sono le seguenti:

- assicurare la memorizzazione in sicurezza e la tracciabilità delle chiamate in entrata;
- assicurare la memorizzazione in sicurezza e la tracciabilità delle chiamate in uscita;
- fornire un ausilio per rilevazioni di tipo quantitativo e statistico;
- per ragioni di giustizia.

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 di 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 gestione delle chiamate siano coerenti e compatibili con le funzioni istituzionali di competenza del Corpo Intercomunale;
- l'utilizzo del sistema di gestione delle chiamate 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 di gestione e il centralino 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, trascorso il periodo di conservazione specificato all'interno del presente regolamento.

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 gestione delle chiamate deve essere configurato per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne 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:

- i tempi di conservazione delle chiamate sia in entrata che in uscita devono essere effettivamente commisurati al reale livello di necessità, evitando la conservazione per tempi indefiniti oppure le conservazione per tempi eccedenti a quelli indispensabili per il perseguimento delle finalità.
- 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 normale" e un profilo più elevato di tipo "administrator";

6.5 Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi, ai sensi dell'art. 11 comma 1 lett. b) del D.Lgs. 196/2003; 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 dall'art. 13 del D.Lgs. 196/2003 (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria). Non sono ammesse finalità generiche o indeterminate, soprattutto quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti.

E' inoltre consentito l'utilizzo delle chiamate registrate 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 – Tipi di trattamenti autorizzati

Nell'installazione e nell'esercizio del sistema di radiolocalizzazione, sono autorizzati esclusivamente le seguenti tipologie di trattamenti:

- installazione e configurazione del centralino telefonico;
- creazione e gestione di gruppi e profili di utenti;
- registrazione di messaggi di benvenuto o di accoglienza;
- fornitura informativa ai sensi art. 13 del D.Lgs. 196/2003;
- registrazione dati relativi alle chiamate in entrata;
- registrazione dati relativi alle chiamate in uscita;
- registrazione chiamate in entrata;
- registrazione chiamate in uscita;
- cancellazione dati relativi alle chiamate in entrata, trascorsi i tempi previsti dal presente regolamento;
- cancellazione dati relativi alle chiamate in uscita, trascorsi i tempi previsti dal presente regolamento;
- cancellazione chiamate in entrata, trascorsi i tempi previsti dal presente regolamento;
- cancellazione chiamate in uscita, trascorsi i tempi previsti dal presente regolamento;
- attivazione trasferimenti di chiamata condizionati ed incondizionati
- consultazione dati e report relativi alle chiamate;
- produzione di report;
- installazione e configurazione di software applicativo;
- installazione e configurazione di software di base;
- installazione di "patch" e "hot fix";
- attivazione collegamenti da remoto;
- 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 un anno in luogo sicuro di files di log.

Art. 8 – 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:

- Titolare del trattamento dei dati;
- Responsabile del trattamento dei dati;
- Responsabile esterno del trattamento dei dati: sono i soggetti (persone fisiche o giuridiche) esterni al Corpo Intercomunale ai quali sono affidati, da parte del Corpo Intercomunale, alcune operazioni di trattamento dei dati e la messa in atto di alcune misure di sicurezza;
- Incaricati del trattamento dei dati: sono i soggetti fisici (persone fisiche) che, designati per iscritto dal titolare o dal responsabile, eseguono una o più operazioni di trattamento dei dati;
- Custode delle password di sistema: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell'amministratore di sistema - delle parole chiave corrispondenti ai vari profili di tipo "administrator" o equivalenti;
- Custode delle parole chiave: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell'incaricato – delle parole chiave assegnate agli utenti finali;
- Soggetti incaricati della gestione e manutenzione degli strumenti elettronici, denominati anche "Amministratori di sistema";
- 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 Vaprio, avrà luogo sotto la diretta responsabilità e titolarità della Pubblica Amministrazione o del soggetto richiedente: sarà pertanto cura 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. 9 – Accesso ai dati da parte del personale di Polizia Locale

Il personale di Polizia Locale diverso dal Comandante e dagli Ufficiali, 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 Comandante e gli Ufficiali potranno accedere ai dati per le finalità succitate e inoltre ai fini di rilevazioni statistiche e per ragioni di giustizia.

Art. 10 – Accesso ai dati da parte dell'Autorità Giudiziaria

Il D.Lgs. 196/2003 prevede (art. 19) che la comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico possa avvenire se:

- prevista da norma di legge o di regolamento, oppure
- anche in assenza di norma di legge o di regolamento, sia necessaria per lo svolgimento delle funzioni istituzionali.

Pertanto l'Autorità Giudiziaria può lecitamente richiedere di:

- accedere ai percorsi georeferenziati;
- accedere ai dati relativi alla radiolocalizzazione ed ottenete 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 nel presente regolamento, ed essere autorizzate dal Sindaco o dal Comandante di Polizia Locale.

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 dal D.Lgs. 196/2003 e più in generale dalla disciplina rilevante in materia di privacy e sicurezza.

Art. 11 – Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento

In generale i soggetti coinvolti nelle operazioni di trattamento dovranno essere designati per iscritto dal titolare 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 e del profilo di accesso dovranno essere oggetto di revisione da parte del responsabile o del titolare con frequenza almeno annuale.

Art. 12 – Tempi di conservazione dei dati relativi alle chiamate

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 alle chiamate potranno essere conservati per un periodo massimo di sei mesi.

E' comunque esplicitamente previsto che i tempi di conservazione dei dati relativi alla radiolocalizzazione possano venire modificati a seguito di variazioni nelle finalità, di mutate esigenze, oppure di motivata richiesta proveniente da altri soggetti pubblici.

Art. 13 – Luogo e modalità di memorizzazione delle dei dati

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" (può essere comunque fatta salva la necessità di una memorizzazione "di backup" su un server remoto). Il suddetto server dovrà essere dedicato esclusivamente alla memorizzazione dei dati relativi alla radiolocalizzazione, e non dovrà essere dedicato ad altri scopi.

Se non diversamente disposto dal titolare con atto scritto, il server non dovrà essere collegato ad internet, oppure dovrà essere collegato solo in casi e per finalità specifiche e ben individuate, per intervalli di tempo il più possibile contenuti.

Non è consentita la memorizzazione "ordinaria" dei dati in locale a livello di postazione "client", o comunque su supporti e strumenti diversi dal succitato server centralizzato. 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 estratte dovrà essere protetta da password e/o criptata.

Art. 14 – 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:

- a livello di software di centrale operativa, deve essere attivato (ed eventualmente configurato) 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 tre mesi;
- il suddetto file di log non dovrà essere per nessun motivo cancellato, modificato o alterato;
- con frequenza al massimo trimestrale, si dovrà procedere all'estrazione (copia) del suddetto file di log;
- la copia estratta del file di log dovrà essere generata in un formato non modificabile (pdf, tiff o altri formati non modificabili) e firmata digitalmente con certificato digitale emesso da una certification authority trusted di primo livello;
- la copia del file di log firmata digitalmente dovrà essere custodita in un luogo sicuro per un periodo di almeno 12 mesi;
- con frequenza trimestrale si dovrà controllare l'operato degli amministratori di sistema, mediante analisi dei file di log e del registro delle operazioni di amministrazione e gestione di sistema effettuate sul sistema di radiolocalizzazione; alla conclusione delle operazioni di controllo / verifica dovrà essere redatto apposito verbale e relazione.

Art. 15 – Requisiti minimi sul luogo di collocazione del server

Il server di memorizzazione dei dati relativi alla radiolocalizzazione dovrà essere collocato all'interno di un locale che fornisca adeguate garanzie di sicurezza fisica e perimetrale. Di seguito si riportano i requisiti minimi che il locale dovrà soddisfare:

- locale ad utilizzo non promiscuo e dedicato esclusivamente a "sala macchine" o "sala server", non agevolmente accessibile al pubblico e ai dipendenti (ad eccezione ovviamente dei dipendenti o collaboratori esplicitamente incaricati di operazioni di amministrazione e gestione di sistema);
- possibilità di regolamentare e di tenere traccia degli accessi al locale;
- locale di norma chiuso a chiave, con serratura e chiave funzionante;
- in caso vi siano finestre a piano terra, presenza di inferriate in ferro non dolce oppure presenza di vetri antisfondamento;
- assenza di carta, cartoni o altro materiale facilmente infiammabile all'interno del locale;
- presenza nelle vicinanze di almeno un estintore non a polvere, funzionante e regolarmente revisionato con frequenza almeno semestrale;
- presenza di adeguato impianto di condizionamento, che assicuri un livello di umidità e temperatura all'interno del range di corretto funzionamento degli apparati.

In aggiunta a quanto elencato, è auspicabile (ancorché non strettamente obbligatoria) la presenza di quanto segue:

- allarme volumetrico (attivato dalla variazione della volumetria all'interno dei locali) o di prossimità;
- presenza di sensori per la rilevazione del fumo e/o della temperatura;
- collegamento dei sensori e dell'allarme con centrale operativa di sicurezza oppure con le forze dell'ordine.

Art. 16 – 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;
- server e client protetti da password iniziale di accesso al programma applicativo; possibilità da parte dell'utente finale di modificare autonomamente le propria password; possibilità di disabilitare (da parte dell'amministratore di sistema) le user-id senza cancellarla;
- presenza di almeno due profili distinti: uno di tipo "administrator" e uno di tipo "utente normale", sia a livello di sistema operativo sia a livello di 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 ai sensi art. 25 del Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003) 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 con frequenza almeno semestrale 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. Di tutto quanto appena elencato si dovrà redigere apposita relazione da discutere con il Comandante della Polizia Locale.

Art. 17 – Notificazione al Garante per la protezione dei dati personali

Stante l'attuale quadro normativo, alla data di ultimo aggiornamento del presente documento non è necessario che i trattamenti effettuati siano notificati al Garante per la protezione dei dati personali, in quanto i trattamenti di dati connessi non rientrano tra i trattamenti previsti dall'art. 37 del D.Lgs. 196/2003.

Art. 18 – 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. 19 – Limiti alla utilizzabilità dei dati personali

La materia è disciplinata dall'art. 14 del D.Lgs. 196/2003.

Art. 20 – Danni cagionati per effetto del trattamento dei dati personali

La materia è disciplinata dall'art. 15 del D.Lgs. 196/2003.

Art. 21 – 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 enti pubblici economici è ammessa unicamente quando prevista da norma di legge o di regolamento.

Art. 22 – Tutela amministrativa e giurisdizionale

Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dalla parte III del D.Lgs. 196/2003.

Art. 23 – Modifiche e integrazioni regolamentari

Il presente regolamento dovrà essere adeguato per recepire eventuali modifiche alla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento alle disposizioni e ai provvedimenti emanati dal Garante per la protezione dei dati personali.

Inoltre, il presente regolamento dovrà venire modificato nel caso dovessero mutare le finalità del sistema di gestione delle chiamate.

Art. 24 – Norme finali

Per quanto non disciplinato dal presente regolamento, si rinvia al Codice in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003, n. 196).

Art. 25 – Pubblicità e conoscibilità del regolamento

Il regime di eventuale pubblicità e conoscibilità del presente regolamento è disciplinato dallo Statuto del Comune di Vaprio d'Adda e dalla disciplina rilevante in materia di accesso agli atti e documenti amministrativi.

Approvato con deliberazione del Consiglio Comunale del Comune di Vaprio d'Adda n. ……..del…….