Città di Grottaferrata

(Città Metropolitana di Roma Capitale)

ALLEGATO 5

Al Regolamento Comunale
per l'attivazione e l'utilizzo
dell'impianto di
videosorveglianza cittadina

ANALISI DEI RISCHI PER I DATI

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

RISCHI: *Si – No*

DESCRIZIONE DELL'IMPATTO SULLA SICUREZZA, gravità: *alta - media – bassa*

Sottrazione di credenziali di autenticazione	Si Media
Carenza di consapevolezza, disattenzione o incuria	Si Media
Comportamenti sleali o fraudolenti o scorretti	Si Alta
Comportamento degli operatori addetti - Errore materiale	Si Bassa
Azione di virus informatici o di programmi suscettibili di recare danno	Si Bassa
Spamming o tecniche di sabotaggio	Si Bassa
Malfunzionamento, indisponibilità o degrado degli strumenti	Si Bassa
Accessi esterni non autorizzati	Si Media
Eventi relativi agli strumenti ed intercettazioni di informazioni in rete	Si Bassa
Accessi non autorizzati a locali/reparti ad accesso ristretto	Si Media
Accessi non autorizzati a strutture e/o armadi contenenti apparati sul territorio comunale	Si Media
Sottrazione di strumenti contenenti dati presso la centrale operativa	Si Bassa
Sottrazione di strumenti contenenti dati presso gli armadi periferici	Si Bassa

Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	Si Bassa	
Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Si Bassa	
Eventi relativi al contesto ed errori umani nella gestione della sicurezza fisica	Si Media	

ADEGUAMENTI E CORRETTIVI, misure da adottare:

- Ai dati personali gestiti possono accedere solo il titolare, i responsabili della gestione tecnica e del trattamento dati e i soggetti da quest'ultimi specificamente incaricati (all'uopo istruiti ed ai quali è consentito un particolare livello di visibilità dei dati, a fronte dei relativi compiti).
- E' prevista l'ammissione fisica ai locali della centrale di controllo con accesso ristretto ai soli autorizzati e con protezione a mezzo di serratura e/o badge, oltre eventuali altri sistemi anti intrusione.
- Gli hardware utilizzati per tale trattamento sono oggetto di manutenzione da parte dell'Ente, anche tramite una competente Società e/o Ditta, nominata all'uopo dal Responsabile tecnico dell'impianto di videosorveglianza, in forza di specifico contratto di servizio.
- L'utilizzo degli hardware/software è soggetto alla digitazione di una password personale, modificata ed aggiornata periodicamente.
- Si prevede l'installazione di un "software sentinella" che protegga gli impianti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale.
- Si prevede l'installazione di un gruppo di continuità (dispositivi UPS) che impedisce danni nel caso di improvvisa assenza di corrente elettrica.
- E' vigente un disciplinare tecnico e di modalità d'uso per il corretto utilizzo del sistema informatico di videosorveglianza, e/o formazione specifica all'uso/utilizzo, che qualsiasi soggetto utilizzatore deve conoscere e rispettare.
- I macchinari informatici sono sottoposti a controlli periodici disposti dal Responsabile tecnico dell'impianto di videosorveglianza ed effettuati dallo stesso e/o dai tecnici competenti nominati, e i programmi del sistema vengono periodicamente aggiornati.
- I software sono dotati di antivirus e di prevenzione malware, e altri eventuali sistemi di salvaguardia e preservazione.
- Si prevede la possibilità dell'adozione di tecniche di cifrature e/o crittografiche e/o separazione identificativa dei dati sensibili trattati.

Come indicato sopra, quali ulteriori misure di sicurezza, in attuazione dell'art. 25 e 32 del Regolamento UE/679/2016, si prevede l'installazione di un "*software sentinella*" che consenta l'immediato rilevamento di indebite intrusioni nella rete, così da adempiere agli obblighi di notifica nei confronti del Garante ed eventualmente dell'interessato di cui agli artt. 33 e 34 del Regolamento UE/679/2016 per i casi di violazione di dati personali.

Le misure adottate, allo stato, risultano tali da prevenire ed attenuare - conformemente alla normativa di settore - i rischi identificati e connessi al trattamento dei dati in oggetto, così evitando rischi elevati per i diritti degli interessati e per le risorse coinvolte nel processo di trattamento dei dati, ai sensi del Regolamento UE 679/2016.