



CAMUGNANO
CASTEL D'AIANO
CASTEL DI CASIO
CASTIGLIONE DEI PEPOLI
GAGGIO MONTANO
GRIZZANA MORANDI
LIZZANO IN BELVEDERE
MARZABOTTO
MONZUNO
SAN BENEDETTO VAL DI SAMBRO
VERGATO

ORIGINALE

**GESTIONE ASSOCIATA DELLE FUNZIONI RELATIVE AI SISTEMI
INFORMATICI E ALLE TECNOLOGIE DELL'INFORMAZIONE**

D E T E R M I N A Z I O N E N R. 680 del 27/07/2018

OGGETTO: RIPRISTINO, POTENZIAMENTO, AGGIORNAMENTO E SERVIZIO DI ASSISTENZA E MANUTENZIONE DEL SISTEMA DI VIDEOSORVEGLIANZA DEL COMUNE DI VERGATO

FIRMATO
IL RESPONSABILE
LEONI EROS

Documento prodotto in originale informatico e firmato digitalmente ai sensi dell'art. 20 del "Codice dell'amministrazione digitale" (D.Leg.vo 82/2005).

L'eventuale stampa del documento costituisce copia analogica sottoscritta con firma a mezzo stampa predisposta secondo l'articolo 3 del D.lgs 12 dicembre 1993, n. 39 e l'articolo 3bis, comma 4bis del Codice dell'amministrazione digitale.

IL RESPONSABILE

Richiamati:

- i provvedimenti presidenziali nr 1/2015 prot. nr. 2572 e nr. 1/2016 prot. nr. 5667, nr. 3/2017 prot. nr. 11543 rispettivamente di nomina del Direttore-Segretario dell'Unione, di nomina dei Responsabili degli uffici e dei servizi, Area delle Posizioni Organizzative, e del Comandante del Servizio Intercomunale di Polizia Municipale, ex artt. 50 e 109, T.U. Enti Locali;
- la deliberazione di Consiglio dell'Unione nr. 3/2018 immediatamente esecutiva recante l'approvazione della nota di aggiornamento del Documento Unico di Programmazione 2018-2020 già approvato con deliberazione di Giunta nr. 56/2017;
- la deliberazione di Consiglio dell'Unione nr. 6/2018 del 19.02.2018 immediatamente esecutiva di approvazione del bilancio di previsione 2018/2020;

Premesso:

- che, con deliberazione del Consiglio dell'Unione nr. 7/2014, veniva approvata la *"Convenzione tra i Comuni di Castel d'Aiano, Castel di Casio, Castiglione dei Pepoli, Gaggio Montano, Grizzana Morandi, Marzabotto, Monzuno, San Benedetto val di Sambro, Vergato e l'Unione di Comuni montani denominata "Unione dei Comuni dell'Appennino bolognese" per il conferimento delle funzioni relative ai sistemi informatici e alle tecnologie dell'informazione (ICT)- approvazione"*
- che la convenzione di conferimento della funzione prevede che annualmente venga approvato il bilancio preventivo di servizio ed il relativo progetto organizzativo funzionale;
- che con l'approvazione del bilancio di previsione 2018-2020 sono stati approvati i bilanci preventivi ed i progetti organizzativi dei servizi gestiti in forma associata;
- che, con deliberazione del consiglio dell'Unione nr. 28/2016, veniva approvata la *"Convenzione per il conferimento all'Unione dei comuni dell'Appennino bolognese delle funzioni di Polizia Municipale e polizia amministrativa locale (art.7 comma 3 lr 21/2012, succ. modif, lr 24/2003, succ. modif, decreto legge n. 78/2010, art. 14, comma 27, lett. i) da parte dei Comuni di Castel d'Aiano, Marzabotto e Vergato;"*
- che, con deliberazione del consiglio dell'Unione nr. 11/2017, veniva approvata la *"Convenzione per il conferimento all'Unione dei comuni dell'Appennino bolognese delle funzioni di Polizia Municipale e polizia amministrativa locale (art.7 comma 3 lr 21/2012, succ. modif, lr 24/2003, succ. modif, decreto legge n. 78/2010, art. 14, comma 27, lett. i) da parte dei Comuni di Monzuno;"*

Rilevati

- la necessità di dotare il territorio gestito dal servizio di Polizia Municipale di un sistema di videosorveglianza, ovvero di riattivare le componenti non più funzionanti dei sistemi esistenti
- le necessità di arrivare ad un sistema che abbia le funzionalità e la copertura analizzate nella documentazione tecnica allegata al presente atto
- la necessità di un censimento dei sistemi e delle infrastrutture attuali che non si limiti alla videosorveglianza, ma che comprenda anche le MAN presenti nel territorio di cui si ha una documentazione frammentaria, che porti ad una conoscenza di dettaglio sufficiente a gestire, in futuro e se opportuno, in modo indipendente le varie componenti del sistema

Visto

- che è possibile procedere alla fornitura tramite procedura negoziata senza previa comunicazione del bando, ai sensi del D.Lgs 50/2016, sia in relazione alla tipologia del servizio che in relazione alla spesa complessiva prevista;
- che la circolare AgID n.2 del 24 giugno 2016, precisando la legge 208/2015 (legge di stabilità 2016), art. 1, commi 512-517, indica l'obbligo da parte delle pubbliche amministrazioni, per procedere all'acquisizione di beni e servizi informatici, di *"ricorrere agli strumenti di acquisto e di negoziazione disponibili presso Consip ed i soggetti aggregatori. Fra i detti strumenti sono ricompresi le convenzioni-quadro, i contratti-quadro e gli accordi-quadro nonché il mercato elettronico della pubblica amministrazione"*
- che la convenzione Consip *"Sistemi di Videosorveglianza e servizi connessi"* è in stato *"Chiuso"* per il *"Lotto 2 Emilia Romagna, Toscana, Lazio, Marche, Abruzzo, Molise, Umbria, Sardegna"*
- le clausole del contratto ritenute essenziali, intese quali operazioni, ripristino e creazione di funzioni che caratterizzano peculiarmente il sistema, il contenuto e i termini entro i quali le prestazioni devono essere eseguite, definite nei documenti tecnici allegati al presente

atto;

- le modalità di scelta del contraente ammesse dalle vigenti disposizioni in materia di contratti delle pubbliche amministrazioni e le ragioni che ne sono alla base;

Ritenuto, pertanto, per la natura della fornitura, di provvedere ad affidare l'analisi, il ripristino, l'estensione, la costruzione e la manutenzione di un *Servizio di videosorveglianza*, come definito nella documentazione tecnica allegata al presente atto, le cui finalità sono riassunte in premessa, stabilendo che:

- la modalità di scelta del contraente è quella della Trattativa diretta con procedura telematica sul portale acquistinretePA.it di Consip, ai sensi del D. Lgs 50/2016
- la scelta della ditta avviene sulla base dei seguenti criteri
 - ditta che opera nella zona del committente in modo da poter rispondere nel modo più celere possibile ad eventuali esigenze imprevedute
 - ditta che ha già operato per il committente sul sistema o su parti di esso, dimostrando le competenze necessarie per svolgere i servizi oggetto della fornitura, in modo da minimizzare i costi e i tempi della fase di assessment, affinché il committente ottenga una conoscenza di dettaglio sufficiente a gestire, in futuro e se opportuno, in modo indipendente le varie componenti del sistema
- sulla base dei criteri precedenti, l'Ente ritiene opportuno avviare la Trattativa diretta con la ditta Mutinanet s.r.l., P.I. 02803360367, sede in Via Imola 90 - 41125 Modena
- la spesa presunta è di 4.000,00 euro per la fase iniziale di rinnovo, sostituzione, potenziamento degli apparati e di € 5.000,00 euro di canone annuo per il servizio di assistenza, esclusa l'IVA di legge
- La spesa, maggiorata dell'IVA di legge, troverà copertura nel bilancio pluriennale secondo le specifiche tecniche dettagliatamente indicate nel successivo atto di affidamento
- la durata prevista del contratto di assistenza è di tre anni, con la possibilità di ulteriori due anni in caso di prolungamento del contratto di manutenzione e assistenza, per un totale di 25.000 euro in 5 anni, oltre l'IVA di legge.
- la forma del contratto sarà quella prevista dal portale acquistinretePA.it di Consip
- le clausole ritenute essenziali sono contenute nel capitolato tecnico allegato al presente atto

Tabella riassuntiva dei costi previsti:

Voce:	Costo €	Costo con IVA (22%) €
Ripristino, rinnovo e potenziamento del sistema con la sostituzione degli apparati inadeguati o obsoleti	4.000,00	4.880,00
Assistenza anno 1	5.000,00	6.100,00
Assistenza anno 2	5.000,00	6.100,00
Assistenza anno 3	5.000,00	6.100,00
Assistenza anno 4 (eventuale)	5.000,00	6.100,00
Assistenza anno 5 (eventuale)	5.000,00	6.100,00
TOTALE	29.000,00	35.380,00

Visti:

- il d.lgs. nr. 267/2000 e s.m.i.
- il d.lgs. 118/2011 e s.m.i. in materia di armonizzazione contabile;
- il d.lgs. 50/2016

D E T E R M I N A

, per le motivazioni esposte in premessa, di:

- procedere alla procedura descritta in premessa, al fine poi di procedere ad affidamento diretto riconducibile alla previsione di cui all'art. 36 comma 2 lettera a), subordinando l'affidamento

medesimo alla positiva verifica dei requisiti nei confronti dell'impresa aggiudicataria e di piena conformità al capitolato tecnico allegato al presente atto;

- precisare, ai sensi dell'art. 192 del D. Lgs. 267/2000 che:
 - il fine che si intende perseguire con il contratto è quello della analisi, il ripristino, l'estensione, la costruzione di nuove componenti e la manutenzione di un Servizio di videosorveglianza, come definito nella documentazione tecnica allegata al presente atto
 - il valore economico massimo del servizio è pari ad € 29.000,00 per 5 anni, comprensiva di spese ed oltre I.V.A. di legge;
 - la stipula del contratto avviene con le modalità previste dal portale acquistinretePA.it di Consip;
 - le clausole ritenute essenziali sono contenute nel capitolato tecnico allegato al presente atto;

di dare atto che:

- il CIG è ZFA2482EA1;
- l'affidatario, ai sensi dell'art. 3 della L. 136/2010 si assumerà, a pena di nullità del contratto, gli obblighi di tracciabilità dei flussi finanziari impegnandosi alla comunicazione del conto corrente dedicato ad appalti/commesse pubbliche di cui al comma 7 del citato articolo;

di approvare la seguente documentazione:

- capitolato tecnico (Progetto) e suoi Allegati

di dare atto che il presente provvedimento è immediatamente efficace non necessitando dell'apposizione del visto di regolarità contabile attestante la copertura finanziaria, ai sensi dell'art. 151 comma 4, T.U. enti locali (D.lgs. 18 agosto 2000, n. 267) e verrà pubblicato all'Albo Pretorio Online dell'Unione dei Comuni per 15 giorni consecutivi.

Il responsabile

Capitolato tecnico

Progetto per la videosorveglianza

1 Stato dell'arte e obiettivi

Nel territorio del Comune di Vergato è presente un sistema di videosorveglianza locale dispiegato nell'area del capoluogo. Molte delle componenti del sistema non sono state sottoposte alla necessaria manutenzione e/o sono comunque diventate obsolete e hanno quindi perso, in parte o completamente, la loro funzionalità. L'allegato "Situazione attuale" riporta lo stato nel dettaglio.

L'Unione dei comuni dell'Appennino bolognese (d'ora in avanti "Ente"), ha quindi elaborato un progetto per la videosorveglianza, attraverso la collaborazione tra il Servizio informatico associato ("SIA") e il Servizio intercomunale di Polizia Municipale.

Obiettivo del progetto è ripristinare, potenziare e rinnovare le componenti esistenti, creando con queste un sistema omogeneo nella fruizione e nelle attività di manutenzione. Inoltre si intende diminuire i consumi elettrici per abbassare i costi di esercizio a carico della PA e per migliorare la sostenibilità ambientale dell'impianto.

Per raggiungere l'obiettivo sopra descritto, l'Ente ritiene opportuno affidare la fornitura dei beni e dei servizi necessari ad un Fornitore specializzato nel settore. La fornitura dovrà rispettare tutte le caratteristiche elencate nel presente Capitolato tecnico.

2 Oggetto della fornitura

Dopo una analisi svolta sul territorio, è risultata necessaria la **sostituzione** della maggior parte degli elementi hardware della infrastruttura attuale; l'offerta dovrà quindi comprendere la fornitura di tutte le videocamere necessarie a sostituire quelle esistenti, due nuovi sistemi di registrazione NVR, oltre a tutti gli interventi che il fornitore riterrà opportuni per sostituire componenti non funzionanti, non compatibili o obsoleti, al fine per raggiungere gli obiettivi definiti.

Devono fare parte dell'offerta anche alcune **modifiche** sui posizionamenti delle videocamere attuali. Gli spostamenti hanno l'obiettivo di ottimizzare il campo di ripresa della videocamera e sgombrarlo dagli

ostacoli che sono venuti a frapporsi nel tempo (segnaletica, rami, ecc.). Gli spostamenti possono essere una semplice modifica dell'orientamento, uno spostamento verso l'alto o il basso sull'attuale palo di installazione o lo scostamento laterale con l'aggiunta di staffe o piccoli pali. La fornitura dovrà comprendere questi spostamenti se sono dell'ordine del metro e riguardano fino ad un massimo di 5 telecamere; eventuali ulteriori esigenze andranno valutate con un accordo separato.

Devono fare parte della fornitura anche l'installazione e la messa in opera di alcuni punti aggiuntivi, indicati nell'allegato "Potenziamenti previsti".

2.1 Caratteristiche minime per il sistema di fruizione

La fruizione, sia in tempo reale sia in differita, delle informazioni raccolte dal sistema deve essere disponibile in maniera distribuita: deve cioè essere possibile visionare i filmati e qualsiasi altra informazione, per il tempo stabilito dalla normativa, da diverse postazioni nella rete informatica dell'Unione, attraverso filtri configurabili legati alla postazione e all'utenza collegata. Deve inoltre essere possibile rendere le informazioni e i filmati disponibili a entità esterne all'Unione che ne abbiano comunque diritto (forze dell'ordine) secondo una procedura tecnica e organizzativa che rispetti la norma vigente. Il sistema deve permettere di impostare filtri e diritti il più possibile dettagliati ed elastici, ad esempio creare profili da assegnare a gruppi di utenti che possano avere l'accesso solo ad alcuni tipi di informazioni, ad alcune parti del sistema, ad un limitato insieme di telecamere, ecc.

Il Fornitore dovrà erogare un servizio di addestramento alla fruizione e alla amministrazione dei sistemi e un servizio di assistenza dedicato agli utilizzatori per tutta la durata del contratto.

2.2 Composizione del sistema

Il sistema ha diverse parti che concorrono al raggiungimento dell'obiettivo. A titolo esemplificativo, ma non esaustivo, si elencano le principali componenti del sistema:

- Videocamere
- Sistema di registrazione e fruizione in rete dei filmati e delle informazioni con storage secondo le norme vigenti
- Apparat per alimentazione elettrica e connessioni di rete (dove dedicati)
- Segnaletica informativa prevista dalle normative vigenti

2.3 Caratteristiche minime delle videocamere

Si richiede che le videocamere abbiano le seguenti caratteristiche minime:

- pieno supporto del protocollo ONVIF
- consumo medio pari o inferiore al 50% del consumo delle telecamere attualmente installate
- risoluzione Full HD
- water-proof e range di temperature tollerate = -20 / +50 °C
- visione notturna
- supporto dei protocolli di rete TCP/IP, UDP, DHCP, NTP, RTSP, DDNS, SMTP, FTP
- interfaccia di rete RJ45

3 Ambito territoriale

L'ambito territoriale è quello del Comune di Vergato.

4 Progettazione

Il progetto finale dovrà garantire le caratteristiche minime descritte in precedenza. Le componenti sostituite e aggiunte al sistema sono di proprietà dell'Ente e il Fornitore è tenuto da subito a condividere con l'Ente tutta la documentazione necessaria e a collaborare con il SIA comunicando per i singoli apparati le seguenti informazioni di minima:

- marca, modello e caratteristiche
- posizionamento
- configurazioni impostate e credenziali amministrative

Altre informazioni potranno essere richieste dal SIA allo scopo di creare una documentazione esaustiva.

5 Manutenzione ordinaria

La manutenzione ordinaria comprende le seguenti attività:

- manutenzione preventiva ossia quella manutenzione eseguita a intervalli predeterminati volta a ridurre la probabilità di guasto o la degradazione del funzionamento;
- manutenzione correttiva che include le azioni volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità, anche attraverso attività di supporto on-site;
- manutenzione evolutiva comprendente tutte le attività inerenti il costante aggiornamento delle componenti software/firmware dei sistemi all'ultima release disponibile sul mercato.

5.1 Manutenzione preventiva

Il servizio di manutenzione preventiva prevede l'obbligo per il Fornitore di effettuare tutti quegli interventi programmati (requisito minimo richiesto 2 volte l'anno, secondo un piano concordato con l'Ente), con personale specializzato presso le sedi dell'Ente ed i luoghi interessati dalla realizzazione del sistema, volti ad evitare l'insorgere di malfunzionamenti. Tali interventi hanno come obiettivo la verifica dello stato di tutti gli elementi facenti parte del servizio, e la eventuale attuazione di tutte le attività finalizzate alla prevenzione di anomalie o guasti.

Tra le attività di manutenzione preventiva possono includersi:

- la verifica e la taratura degli apparati installati (ad esempio l'orientamento delle telecamere ed apparati wireless);
- la pulizia delle ottiche e la lubrificazione delle parti mobili;
- la sostituzione di parti di ricambio e parti soggette ad usura, atte a prevenire e a ridurre i guasti e a mantenere in condizioni di adeguata funzionalità le apparecchiature oggetto del presente appalto;
- la verifica periodica della rispondenza dell'apparecchiatura alle specifiche di funzionamento previste dal costruttore.

5.2 Manutenzione correttiva

Più in dettaglio le attività di manutenzione correttiva possono riassumersi in:

- risoluzione del problema tramite indicazione telefonica all'utente o eventuale intervento remoto;
- risoluzione della causa del guasto tramite, ove necessario:
- intervento presso la sede/luogo interessato;
- sostituzione di parti o di interi apparati finalizzate al recupero delle prestazioni iniziali dell'apparecchiatura ovvero correzione di bug software;

- ripristino del servizio sui livelli preesistenti al guasto/anomalia;
- collaudo del sistema per verificare l'eliminazione della causa del guasto;
- ritiro presso i siti di installazione degli apparati guasti, o parti di essi, per i quali è stato diagnosticato un guasto o richiesto l'intervento, e riconsegna e messa in opera degli stessi riparati. Gli apparati sostitutivi e le parti di ricambio dovranno essere della stessa marca, modello e tipo e nuove di fabbrica. Nel caso di servizio di manutenzione dell'esistente, il Fornitore potrà prevedere la sostituzione con apparati e parti di ricambio equivalenti;
- in caso di indisponibilità delle parti di ricambio o per qualsiasi altra causa non imputabile all'Ente, il Fornitore avrà la facoltà di sostituire, interamente e a proprie spese, il dispositivo guasto con uno sostitutivo di prestazioni analoghe o superiori (in tal caso sarà necessario concordare tale evenienza con l'Ente);
- aggiornamento della documentazione relativa;
- redazione del relativo "verbale di intervento".

Sono inclusi nel servizio anche gli interventi e gli oneri dovuti a guasti o malfunzionamenti causati da:

- sovratensione;
- sovracorrente;
- sovratemperatura;

mentre sono esclusi gli oneri dovuti a guasti o malfunzionamenti causati da:

- uso non conforme degli apparati/sistemi;
- atti dolosi e vandalici;
- eventi accidentali (ad. esempio abbattimento di palo di sostegno a seguito di incidente stradale);
- incendio per cause esterne e danneggiamenti da opere di spegnimento;
- allagamenti o inondazioni;
- caduta di fulmini.

È previsto l'obbligo per il Fornitore di operare con personale specializzato presso la sede dell'Ente in cui si sia verificata il malfunzionamento. Il personale del Fornitore coinvolto deve avere adeguate qualifiche professionali in termini di conoscenza specifica delle attività e tecnologia, attestata tramite certificazioni ovvero esperienza lavorativa almeno triennale in ambito manutenzione e gestione di sistemi di videosorveglianza. Qualora il Fornitore stimasse che il tempo per la risoluzione dei problemi sia maggiore a quello definito dai livelli di servizio, sarà tenuto a proporre procedure alternative per consentire il temporaneo funzionamento del sistema, sino al ripristino completo dello stesso. Tali procedure saranno valutate ed approvate dall'Ente. Gli interventi dovranno concludersi con l'attività di verifica del corretto funzionamento delle apparecchiature sostituite o riparate e del sistema nella sua globalità; tale verifica sarà a cura del Fornitore, ma è lasciata libertà all'Ente di coinvolgere proprio personale e/o personale di terzi. Il Fornitore è tenuto al rispetto delle modalità operative ed al rilascio della documentazione prevista dalla normativa vigente.

5.3 Manutenzione evolutiva

Il servizio di manutenzione evolutiva prevede l'obbligo per il Fornitore di effettuare tutte le attività inerenti il costante aggiornamento delle componenti software/firmware dei sistemi all'ultima release disponibile sul mercato. Il Fornitore si impegna a monitorare costantemente il rilascio di aggiornamenti (o correzioni di eventuali bug) del software/firmware dei sistemi inseriti nel contratto di manutenzione e dovrà provvedere al deployment del nuovo software/firmware sui sistemi interessati.

6 Livelli di servizio e qualità (Service level agreement)

I Service Level Agreement (SLA) definiscono i parametri di qualità del servizio che devono essere rispettati dal Fornitore. Per ciascuno di tali parametri è stabilita una Soglia Richiesta al superamento della quale scatterà il meccanismo di applicazione delle relative penali descritte nel paragrafo dedicato. Tranne ove espressamente specificato, i valori dei parametri di SLA descritti nei paragrafi seguenti saranno misurati in riferimento alla finestra temporale di erogazione dei servizi

Lun-Ven 8.00 - 17.00 e Sab 8.00-14.00

Relativamente ai servizi di assistenza, manutenzione e gestione, i guasti segnalati al Call Center del Fornitore saranno codificati secondo una classe di severità (Severity Code), in base alla gravità del problema riscontrato. Sulla base del Severity Code assegnato il Call Center dovrà fornire una stima dei tempi di ripristino e delle modalità di intervento nel rispetto dei parametri di SLA nel seguito definiti, eventualmente avvalendosi della possibilità di effettuare una prima diagnosi da remoto.

I Severity Code sono

1. Severity Code 1 = Guasto Bloccante: le funzionalità di base e/o maggiormente rilevanti non sono più operative.
2. Severity Code 2 = Disservizio: le funzionalità di base sono operative ma il loro utilizzo non è soddisfacente.

6.1 SLA per la consegna, installazione e avvio dei servizi

Le attività di fornitura, installazione e relative verifiche funzionali effettuate dal Fornitore, saranno monitorate sulla base dei seguenti parametri di SLA:

- Tempo di consegna, installazione e verifica: è definito come il tempo, misurato in giorni solari, che intercorre tra la data in cui si formalizza la necessità di una fornitura di materiale in base al progetto e la data riportata sul “Verbale di Fornitura” in cui si accerta la corretta messa in esercizio;
- Tempo di avvio dei servizi: è definito come il tempo, misurato in giorni solari, che intercorre tra la data di stipula del contratto di servizio e la data di comunicazione di presa in carico dei sistemi e avvio dei servizi riportata nella “Lettera di avvio del servizio”.

Il Fornitore dovrà effettuare la fornitura, l’installazione e le verifiche funzionali degli apparati, hardware e software, entro i tempi massimi di seguito indicati, salvo diverso accordo tra le parti risultante o dal cronoprogramma riportato nel progetto esecutivo approvato, in ogni caso decorrenti dall’ordinativo di fornitura:

- Tempo di consegna, installazione e verifica: 55 giorni solari
- Tempo di avvio dei servizi: 50 giorni solari

6.2 SLA per le attività di supporto al collaudo

Le attività di supporto al collaudo (a carico del Fornitore) effettuato dall’Ente, saranno monitorate sulla base dei seguenti parametri di SLA:

- Predisposizione secondo collaudo: è definito come il tempo, misurato in giorni solari, che intercorre tra la data riportata sul “Verbale di Collaudo” relativo al primo, eventuale, collaudo negativo e la data della comunicazione della disponibilità all’effettuazione del secondo collaudo;
- (Eventuale, ad esclusiva discrezione dell’Ente) Predisposizione terzo collaudo: è definito come il tempo, misurato in giorni solari, che intercorre tra la data riportata sul “Verbale di Collaudo” relativo al secondo collaudo negativo e la “Data di accettazione” riportata sul “Verbale di Collaudo” (in caso di ulteriore collaudo positivo).

Per queste attività si prevedono i tempi seguenti:

- Predisposizione secondo collaudo: 15 giorni solari
- (Eventuale, ad esclusiva discrezione dell’Ente) Predisposizione terzo collaudo: 10 giorni solari

6.3 SLA per i servizi di assistenza e manutenzione del nuovo e dell’esistente

Di seguito sono elencati i Service Level Agreement che il Fornitore dovrà soddisfare relativamente ai servizi di assistenza e manutenzione del nuovo e dell’esistente.

- Tempestività di risposta al disservizio: è definita come lo scostamento, misurato in ore, tra il tempo misurato ed i valori target in relazione alla segnalazione del disservizio da parte dell’Ente e la comunicazione, da parte dell’operatore del Call Center, della diagnosi di massima del disservizio e previsione su modalità e tempistiche di ripristino (compreso il Severity Code assegnato).
- Tempestività del tempo di intervento: è definita come lo scostamento, misurato in ore, tra il tempo misurato ed i valori target in relazione alla segnalazione del disservizio da parte dell’Ente e l’intervento, qualora necessario, presso la sede interessata a cura del personale tecnico messo a disposizione dal Fornitore.
- Tempestività del tempo di ripristino del servizio: è definita come lo scostamento, misurato in giorni, tra il tempo misurato ed i valori target in relazione alla segnalazione del disservizio da parte dell’Ente e la risoluzione dello stesso.

I tempi per le azioni sopra elencate dipendono dal Severity Code del disservizio individuato e sono riportati nella tabella seguente

Azione	Tempi previsti	
	Severity Code 1	Severity Code 2
Risposta al disservizio	8 ore	
Intervento	8 ore lavorative*	36 ore lavorative*
Ripristino	2 giorni lavorativi*	5 giorni lavorativi*

* salvo diverso accordo tra le parti per casi specifici

7 Monitoraggio della qualità erogata

L'Ente si riserva la facoltà di attivare funzioni di monitoraggio della qualità del progetto e del servizio erogato.

Al fine del monitoraggio dei livelli di servizio da parte dell'Ente, il Fornitore dovrà approntare un sistema informativo di monitoraggio che sia in grado di collezionare con aggiornamento settimanale tutti i dati rilevanti ai fini del calcolo degli Indicatori di Qualità mantenendo uno storico degli stessi. Tali dati dovranno essere resi integralmente disponibili su richiesta da parte dell'Ente o azienda esterna autorizzata da essa, che potrà in particolare richiedere l'emissione di rapporti contenenti i valori aggiornati degli indicatori di qualità.

Nel corso dell'esercizio sarà effettuato, da parte dell'Ente o azienda esterna autorizzata da essa, un monitoraggio periodico o a campione delle modalità di progettazione e di erogazione dei servizi al fine di verificare il rispetto dei parametri prescritti. Il Fornitore si impegna in ogni caso a risolvere quelle condizioni di ridotta qualità che possono creare problemi all'Ente.

Il Fornitore, nel prendere atto di quanto espresso, dovrà rendere disponibile tutta la necessaria collaborazione attraverso la fornitura tempestiva dei dati necessari (su supporto informatico). L'Ente si riserva di effettuare tutte le verifiche che riterrà opportune, addebitandone al Fornitore i relativi costi nel caso esse dimostrino la non completezza o correttezza dei dati ricevuti.

8 Penali sui livelli di servizio

In caso di mancato rispetto dei parametri di SLA richiesti nel presente Documento e in relazione a quanto espresso nelle sezioni precedenti, il Fornitore sarà tenuto a corrispondere all'Ente, le penali di seguito riepilogate fatto salvo, in ogni caso, il risarcimento del maggior danno subito.

Azione	Valore target	Penale
Tempi di consegna, installazione e verifica	55 giorni solari o diverso valore indicato nel progetto approvato dall'Ente	0,1% del valore totale dell'appalto per ogni giorno solare di ritardo
Tempi di consegna, installazione e verifica	50 giorni solari o diverso valore indicato nel progetto approvato dall'Ente	0,1% del valore totale dell'appalto per ogni giorno solare di ritardo
Predisposizione di eventuali collaudi successivi ad un collaudo negativo	15 giorni solari dal collaudo precedente	0,1% del valore totale dell'appalto per ogni giorno solare di ritardo
Attivazione del servizio di assistenza tramite call center	15 giorni solari dalla attivazione del servizio	50 euro per ogni giorno solare di ritardo
Tempestività per i servizi di assistenza e manutenzione	Come da tabella del paragrafo 6.3	50 euro per ogni giorno di ritardo per i disservizi con Severity Code 2; 100 euro per ogni giorno di ritardo per i disservizi con Severity Code 1

L'Ente si riserva di non esigere le penali per i casi specifici dove non lo ritenga opportuno.

Le penali saranno richieste con comunicazione formale via PEC al Fornitore; il Fornitore avrà 10 giorni solari di tempo per eventuali controdeduzioni.

9 Designazione quale responsabile del trattamento dei dati personali ai sensi del Regolamento U.E. 679/2016

In esecuzione del presente contratto, il Fornitore effettua trattamento di dati personali di titolarità dell'Ente. In virtù di tale trattamento, le Parti stipulano l'accordo allegato al fine di disciplinare oneri e responsabilità in aderenza al Regolamento (UE) del Parlamento e del Consiglio europeo n. 2016/679 (di seguito, anche "GDPR") e da ogni altra normativa applicabile.

Il Fornitore è, pertanto, designato dall'Ente quale Responsabile esterno del trattamento dei dati personali ai sensi e per gli effetti dell'art. 28 del Regolamento per i trattamenti dei dati rilevati e gestiti dal sistema di videosorveglianza oggetto del contratto. Il Fornitore si obbliga a dare esecuzione al contratto suindicato conformemente a quanto previsto dall'Accordo allegato al presente contratto.

Le Parti riconoscono e convengono che il rispetto delle istruzioni di cui all'accordo allegato, nonché alle prescrizioni della normativa applicabile, non producono l'insorgere di un diritto in capo al Responsabile esterno del trattamento al rimborso delle eventuali spese che lo stesso potrebbe dover sostenere per conformarsi.

10 Sicurezza e riservatezza

Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e comunque a conoscenza, anche tramite l'esecuzione del contratto, di non divulgarli in alcun modo e in qualsiasi forma, di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del Contratto e di non farne oggetto di comunicazione o trasmissione senza l'espressa autorizzazione dell'Ente.

L'obbligo di cui sopra sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione del Contratto, fatta esclusione per i dati che siano o divengano di pubblico dominio.

Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché di subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza definiti sopra e risponde nei confronti della Committente per eventuali violazioni dell'obbligo di riservatezza commesse dai suddetti soggetti.

Il Fornitore può utilizzare servizi di cloud pubblici ove memorizzare i dati e le informazioni trattate nell'espletamento dell'incarico affidato, solo previa autorizzazione dell'Ente.

In caso di inosservanza degli obblighi descritti nel presente articolo, l'Ente ha facoltà di dichiarare risolto di diritto il Contratto, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che ne dovessero derivare.

Il Fornitore potrà citare i termini essenziali del Contratto nei casi in cui fosse condizione necessaria per la partecipazione del Fornitore stesso a gare e appalti, previa comunicazione all'Ente delle modalità e dei contenuti di detta citazione.

Sarà possibile ogni operazione di auditing da parte dell'Ente attinente le procedure adottate dal Contraente in materia di riservatezza e degli altri obblighi assunti dal presente contratto.

Il Fornitore non potrà conservare copia di dati e programmi dell'Ente, né alcuna documentazione inerente ad essi dopo la scadenza del Contratto e dovrà, su richiesta, ritrasmetterli all'Ente.

Indice generale

1 Stato dell'arte e obiettivi.....	1
2 Oggetto della fornitura.....	1
2.1 Caratteristiche minime per il sistema di fruizione.....	2
2.2 Composizione del sistema.....	2
2.3 Caratteristiche minime delle videocamere.....	2
3 Ambito territoriale.....	2
4 Progettazione.....	3
5 Manutenzione ordinaria.....	3
5.1 Manutenzione preventiva.....	3
5.2 Manutenzione correttiva.....	3
5.3 Manutenzione evolutiva.....	4
6 Livelli di servizio e qualità (Service level agreement).....	5
6.1 SLA per la consegna, installazione e avvio dei servizi.....	5
6.2 SLA per le attività di supporto al collaudo.....	5
6.3 SLA per i servizi di assistenza e manutenzione del nuovo e dell'esistente.....	6
7 Monitoraggio della qualità erogata.....	7
8 Penali sui livelli di servizio.....	7
9 Designazione quale responsabile del trattamento dei dati personali ai sensi del Regolamento U.E. 679/2016.....	8
10 Sicurezza e riservatezza.....	8

ALLEGATI

- Situazione attuale
- Potenziamanti previsti
- Accordo per il trattamento dei dati personali

Allegato Accordo per il trattamento di dati personali

Il presente accordo costituisce allegato parte integrante del contratto siglato tra l'Ente Unione dei comuni dell'Appennino bolognese (d'ora in avanti "Ente"), Titolare del trattamento dei dati personali, e il Fornitore di servizi, designato Responsabile esterno del trattamento di dati personali ai sensi dell'art. 28 del GDPR.

1. Premesse

Il presente Accordo si compone delle clausole di seguito rappresentate e dalle seguenti Appendici, che ne formano parte integrante e sostanziale:

- Appendice 1: Glossario
- Appendice 2: Security

Le Parti convengono quanto segue:

2. Trattamento dei dati nel rispetto delle istruzioni dell' Ente

2.1 Il Fornitore, relativamente a tutti i Dati personali che tratta per conto dell'Ente garantisce che:

- tratta tali Dati personali solo ai fini dell'esecuzione dell'oggetto del contratto, e, successivamente, solo nel rispetto di quanto eventualmente concordato dalle Parti per iscritto, agendo pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dall'Ente;
- non trasferisce i Dati personali a soggetti terzi, se non nel rispetto delle condizioni di liceità assolute dall'Ente e a fronte di quanto disciplinato nel presente accordo;
- non tratta o utilizza i Dati personali per finalità diverse da quelle per cui è conferito l'incarico dall'Ente, financo per trattamenti aventi finalità compatibili con quelle originarie;
- prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà l'Ente se, a suo parere, una qualsiasi istruzione fornita dall'Ente si ponga in violazione di Normativa applicabile;

2.2. Al fine di dare seguito alle eventuali richieste da parte di soggetti interessati, il Fornitore si obbliga ad adottare:

- procedure idonee a garantire il rispetto dei diritti e delle richieste formulate all'Ente dagli interessati relativamente ai loro dati personali;
- procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta dell'Ente dei dati personali di ogni interessato;
- procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali a richiesta dall'Ente;
- procedure atte a garantire il diritto degli interessati alla limitazione di trattamento, su richiesta dell'Ente.

2.3 Il Responsabile del trattamento deve garantire e fornire all'Ente cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente richieste dalla stessa, per consentirle di adempiere ai propri obblighi ai sensi della normativa applicabile, ivi compresi i provvedimenti e le specifiche decisioni del Garante per la protezione dei dati personali.

2.4 Il Responsabile del trattamento, anche nel rispetto di quanto previsto all'art. 30 del Regolamento, deve mantenere, compilare e rendere disponibile a richiesta della stessa, un registro dei trattamenti dati personali che riporti tutte le informazioni richieste dalla norma.

2.5 Il Responsabile del trattamento assicura la massima collaborazione al fine dell'esperimento delle valutazioni di impatto ex art. 35 del GDPR che l'Ente intenderà esperire sui trattamenti che rivelano, a Suo insindacabile giudizio, un rischio elevato per i diritti e le libertà delle persone fisiche.

3. Le misure di sicurezza

3.1 Il Responsabile del trattamento deve conservare i dati personali garantendo la separazione di tipo logico dai dati personali trattati per conto di terze parti o per proprio conto.

3.2 Il Responsabile del trattamento deve adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati, ed in particolare, laddove il trattamento comporti trasmissioni di dati su una rete, da qualsiasi altra forma illecita di trattamento.

3.3 Il Responsabile del trattamento conserva, nel caso siano allo stesso affidati servizi di amministrazione di sistema, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;

3.4 L'Ente attribuisce al Responsabile del trattamento il compito di dare attuazione alla prescrizione di cui al punto 2 lettera e) "Verifica delle attività" del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

3.5 Il Responsabile del trattamento deve adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti all'Ente, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.

3.6 Il Responsabile del trattamento adotta le misure di sicurezza di cui all'Appendice "Security" allegata al presente accordo. In ragione della riservatezza delle evidenze di analisi di conformità alle misure di cui alla suddetta Appendice, il Fornitore condivide con l'Ente tali informazioni solo in caso di violazione o data breach. Si sottolinea che, ad ogni buon conto, la sottoscrizione del presente accordo, e dei suoi allegati, equivale ad attestazione della conformità del Responsabile, e della soluzione informatica prodotta/sviluppata, alle misure indicate nell'appendice "Security".

4. Analisi dei rischi, privacy by design e privacy by default

4.1 Con riferimento agli esiti dell'analisi dei rischi effettuata dall'Ente sui trattamenti di dati personali cui concorre il Fornitore, lo stesso assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dall'Ente per affrontare eventuali rischi identificati.

4.2 Il Fornitore dovrà consentire all'Ente, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo trattamento, di adottare, sia nella fase iniziale di determinazione dei mezzi di trattamento, che durante il trattamento stesso, ogni misura tecnica ed organizzativa che si riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.

4.3 In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento, e che in particolare non siano accessibili dati personali ad un numero indefinito di soggetti senza l'intervento di una persona fisica.

4.4 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle policy di privacy by design e by default adottate dall'Ente e specificatamente comunicate.

5. Soggetti autorizzati ad effettuare i trattamenti - Designazione

5.1 Il Responsabile del trattamento garantisce competenze ed affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali (di seguito anche incaricati) effettuati per conto dell'Ente.

5.2 Il Responsabile del trattamento garantisce che gli incaricati abbiano ricevuto adeguata formazione in materia di protezione dei dati personali e sicurezza informatica, consegnando all'Ente le evidenze di tale formazione.

5.3 Il Responsabile del trattamento, con riferimento alla protezione e gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza non meno onerosi di quelli previsti nel Contratto di cui il presente documento costituisce parte integrante. In ogni caso il Fornitore sarà direttamente ritenuto responsabile per qualsiasi divulgazione di dati personali dovesse realizzarsi ad opera di tali soggetti.

6. Sub-Responsabili del trattamento di dati personali

6.1 Il Fornitore, nell'eventualità di subappalto occorso ai sensi della normativa in materia di appalti e, per tutte le evenienze, nei casi di conferimento di parte del trattamento dei dati personali a soggetti terzi sub-responsabili, impone agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nel presente Accordo.

6.2 Su specifica richiesta dell'Ente, il Fornitore dovrà provvedere a che ogni Sub-Responsabile sottoscriva direttamente con l'Ente un accordo di trattamento dei dati che, a meno di ulteriori e specifiche esigenze, preveda sostanzialmente gli stessi termini del presente Accordo.

6.3 In tutti i casi, il Fornitore si assume la responsabilità nei confronti dell'Ente per qualsiasi violazione od omissione realizzati da un Sub-Responsabile o da altri terzi soggetti incaricati dallo stesso,

indipendentemente dal fatto che il Fornitore abbia o meno rispettato i propri obblighi contrattuali, ivi comprese le conseguenze patrimoniali derivanti da tali violazioni od omissioni.

7. Trattamento dei dati personali fuori dall'area economica europea

7.1 L'Ente non autorizza il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea.

8. Cancellazione dei dati personali

8.1 Il Fornitore provvede alla cancellazione dei dati personali trattati per l'esecuzione del presente contratto al termine del periodo di conservazione e in qualsiasi circostanza in cui sia richiesto dall'Ente, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte di interessati.

8.2 Alla cessazione del Contratto e, conseguentemente del presente Accordo, per qualsiasi causa avvenga, i dati personali dovranno, a discrezione dell'Ente, essere distrutti o restituiti alla stessa, unitamente a qualsiasi supporto fisico o documento contenente dati personali di proprietà dell'Ente.

9. Audit

9.1 Il Fornitore si rende disponibile a specifici audit in tema di privacy e sicurezza informatica da parte dell'Ente.

9.2 Il Fornitore consente, pertanto, all'Ente l'accesso ai propri locali e ai locali di qualsiasi Sub-Responsabile, ai computer e altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che il Fornitore, e/o i suoi Sub-fornitori, rispettino gli obblighi derivanti dalla normativa in materia di protezione dei dati personali e, quindi, da questo Accordo.

9.3 L'esperimento di tali audit non deve avere ad oggetto dati di terze parti, informazioni sottoposte ad obblighi di riservatezza degli interessi commerciali.

9.4 Nel caso in cui l'audit fornisca evidenze di violazioni alla normativa in materia di protezione dei dati personali e al presente Accordo, quali ad esempio quelle indicate all'art. 83 comma 5 (con esclusione della lett. e) l'Ente può risolvere il Contratto o chiedere una cospicua riduzione del prezzo.

9.5 Nel caso in cui l'audit fornisca evidenze di violazioni gravi, quali ad esempio quelle indicate all'art. 83 comma 4 lett. a), l'Ente può chiedere una cospicua riduzione del prezzo.

9.6 Il rifiuto del Fornitore di consentire l'audit all'Ente comporta la risoluzione del contratto.

10. Indagini dell'Autorità e reclami

Nei limiti della normativa applicabile, il Fornitore o qualsiasi Sub-Responsabile informa senza alcun indugio l'Ente di qualsiasi:

- richiesta o comunicazione promanante dal Garante per la protezione dei dati personali o da forze dell'ordine;

- istanza ricevuta da soggetti interessati.

Il Fornitore fornisce, in esecuzione del contratto e, quindi, gratuitamente, tutta la dovuta assistenza all'Ente per garantire che la stessa possa rispondere a tali istanze o comunicazioni nei termini temporali previsti dalla normativa e dai regolamentari applicabili.

11. Violazione dei dati personali e obblighi di notifica

11.1 Il Fornitore, in virtù di quanto previsto dall'art. 33 del Regolamento, dovrà comunicare a mezzo di posta elettronica certificata all'Ente nel minor tempo possibile, e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione di sicurezza che abbia comportato 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, ivi incluse quelle che abbiano riguardato i propri sub-Fornitori. Tale comunicazione deve contenere ogni informazione utile alla gestione del *data breach*, oltre a:

- descrivere la natura della violazione dei dati personali;
- le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- i recapiti del DPO nominato o del soggetto competente alla gestione del data breach;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o che si intende adottare per affrontare la Violazione della sicurezza, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi.

11.2 Il Fornitore deve fornire tutto il supporto necessario all'Ente ai fini delle indagini e sulle valutazioni in ordine alla violazione di dati, anche al fine di individuare, prevenire e limitare gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo con l'Ente, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa. Il Fornitore non deve rilasciare, né pubblicare alcun comunicato stampa o relazione riguardante eventuali data breach o violazioni di trattamento senza aver ottenuto il previo consenso scritto dell'Ente.

12. Responsabilità e manleve

12.1 Il Fornitore tiene indenne e manleva l'Ente da ogni perdita, costo, sanzione, danno e da ogni responsabilità di qualsiasi natura derivante o in connessione con una qualsiasi violazione da parte del Fornitore delle disposizioni contenute nel presente Accordo.

12.2 A fronte della ricezione di un reclamo relativo alle attività oggetto del presente Accordo, il Fornitore:

- avverte, prontamente ed in forma scritta, l'Ente del Reclamo;
- non fornisce dettagli al reclamante senza la preventiva interazione con l'Ente;
- non transige la controversia senza il previo consenso scritto dell'Ente;

- fornisce all'Ente tutta l'assistenza che potrebbe ragionevolmente richiedere nella gestione del reclamo.

Appendice I

GLOSSARIO

“Garante per la protezione dei dati personali”: è l’autorità di controllo responsabile per la protezione dei dati personali in Italia;

“Dati personali ”: qualsiasi 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 a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

“GDPR” o “Regolamento”: si intende il Regolamento UE 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e della loro libera circolazione (General Data Protection Regulation) che sarà direttamente applicabile dal 25 maggio 2018;

“Normativa Applicabile”: si intende l’insieme delle norme rilevanti in materia protezione dei dati personali , incluso il Regolamento Privacy UE 2016/679 (GDPR) ed ogni provvedimento del Garante per la protezione dei dati personali e del WP Art. 29.

“Appendice Security”: consiste nelle misure di sicurezza che il Titolare determina assicurando un livello minimo di sicurezza, e che possono essere aggiornate ed implementate dal Titolare, di volta in volta, in conformità alle previsioni del presente Accordo;

“Reclamo”: si intende ogni azione, reclamo, segnalazione presentata nei confronti del Titolare o di un Suo Responsabile del trattamento;

“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 tale trattamento sono determinati dal diritto dell'Unione 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;

“Trattamento”: qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi 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;

“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

“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.

Appendice 2

Security

L'Ente deve adottare le misure minime per la sicurezza ICT stabilite da AGID con la circolare del 18 aprile 2017, n. 2/2017 pubblicata sulla Gazzetta Ufficiale, al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi.

Tali misure sono descritte all'indirizzo: <https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict>

ALLEGATO Situazione attuale**Vergato capoluogo****Sistema di registrazione e fruizione delle informazioni (DVR, NVR, ...)****Registrazione non funzionante****Videocamere**

id	posizione	tipo	marca/modello	raggiungibile	problemi
101	Piazza Capitani della Montagna-zona centrale della piazza	dome	WV-NW960-Panasonic	ok	sporca
102	via cavour all'altezza del plesso scolastico	dome	WV-NW960-Panasonic	ok	sporca
103	Piazza Giovanni XXIII-parcheggio FS lato Buffet	dome	WV-NW960-Panasonic	ok	sporca
104	Via Marconi-intersezione con Via Garibaldi	dome	WV-NW960-Panasonic	ok	sporca
105	Via Bortolotti-intersezione Piazza IV novembre/Via Buriani	dome	WV-NW960-Panasonic	ok	sporca
106	Discarica	dome	WV-NW960-Panasonic	ok	sporca
121	Via Berlinguer-in angolo con il Parco Giochi	dome	WV-NW960-Panasonic	instabile	sporca
122	Via Berlinguer-rotatoria con vista su Via Pertini e su Via della Repubblica,oltre che sulla parte iniziale della stessa Via Berlinguer	dome	WV-NW960-Panasonic	ok	sporca
123	Galleria 1 maggio-interno del centro commerciale	dome	WV-NW960-Panasonic	ok	sporca
124	Galleria 1 maggio-interno del centro commerciale	dome		ko	non funziona
125	Piazza XXV aprile-intersezione Galleria 1 maggio	dome		ko	non funziona
151	Piazza Capitani della Montagna-ingresso del Municipio	fissa		ko	non funziona
152	Piazza Capitani della Montagna-ingresso del Municipio	fissa	WV-NP1000-Panasonic	ok	
153	Via Garibaldi-civico 17,verso Via Di Vittorio	fissa	WV-NP1000-Panasonic	ok	sporca
154	Piazza della Pace-verso Via Garibaldi	fissa	WV-NP1000-Panasonic	ok	
155	Piazza della Pace-Ingrosso della mensa Asilo Nido	fissa		ko	non funziona
156	Piazza della Pace-Unione dei comuni,verso sagrato Chiesa	fissa		ko	non funziona
157	Parco giochi Piazza della Pace	fissa	WV-NP1000-Panasonic	ok	sporca
158	Via Marconi-Asilo Nido,viale giardini	fissa	WV-NP1000-Panasonic	ok	alberi ostruiscono la visuale
159	via Comani – Repubblica verso BO	fissa		ko	non funziona
160	Via Minghetti – Costituzione verso PT			ko	non funziona
161	Via Roma – Costituzione 1			ko	non funziona

Vergato

162	Via Roma – Costituzione 2			ko	non funziona
163	Via Minghetti – Costituzione verso BO			ko	non funziona
164	via Comani – Repubblica verso PT	fissa		ko	non funziona
165	intersezione via fornaci – via botrolotti SS64 verso PT	fissa	WV-NP240-Panasonic	ok	
166	intersezione via fornaci – via botrolotti SS64 verso BO	fissa	WV-NP240-Panasonic	ok	palo che ostruisce parte della visuale
167	Via della Repubblica-intersezione Via Rimembranze, posizionata nelle due direttrici di marcia SS64	fissa	WV-NP240-Panasonic	ok	
169	Discarica 2	fissa	WV-SP306-Panasonic	ok	
170	Discarica 1	fissa	WV-SP306-Panasonic	ok	
171	Via della Repubblica-intersezione Via Rimembranze, posizionata nelle due direttrici di marcia SS64	fissa	WV-NP240-Panasonic	ok	sporca

ALLEGATO Potenzamenti previsti

Vergato capoluogo

Videocamere

posizione

Piazza della stazione ferroviaria – sito di installazione della fontana di Ontani

Piazza dei Capitani orientata e zoomata sull'ingresso da Via Cavour

Zona Fornaci – complesso casa protetta, centro diurno, centro sociale e centro documentazione