Fornitura di telecamere (body-cam) per il personale di Polizia penitenziaria - Dipartimento Amministrazione Penitenziaria - Avviso di consultazione preliminare di mercato n. 8193.ID

24 marzo 2023

Dipartimento dell'amministrazione penitenziaria
Direzione generale per la gestione dei beni, dei servizi e degli interventi in materia di edilizia penitenziaria

Prot. n. 8193.ID del 24 marzo 2023

Avviso di consultazione preliminare di mercato ex art. 66 d.lgs. 50/2016, in aderenza alle linee guida n. 8 e n. 14 dell'A.N.A.C., per l'affidamento della fornitura e posa in opera di un sistema di telecamere (body-cam) per il personale del Corpo di polizia penitenziaria.

1. Premessa

Il Ministero della Giustizia- Dipartimento dell'Amministrazione Penitenziaria ha l'esigenza di dotare il Corpo di polizia penitenziaria di un sistema di telecamere indossabili (body-cam), ossia di apparati di registrazione audio-video portatile da utilizzare nello svolgimento delle attività di servizio relative alla tutela dell'ordine e della sicurezza svolte nell'ambito dell'espletamento dei compiti istituzionali nelle diverse sedi decentrate dislocate su tutto il territorio nazionale.

2. Dettaglio Tecnico richiesto

Il sistema deve consentire di acquisire registrazioni audio e video nonché singole immagini in modalità foto. La videocamera non deve essere dotata di display LCD e, pertanto, non deve essere possibile la visualizzazione delle registrazioni direttamente sull'apparato.
La "memoria" deve essere integrata nella videocamera e perciò non può essere rimovibile. In caso di spegnimento per batteria scarica o di spazio di memorizzazione esaurito, l'apparato provvede al salvataggio automatico della registrazione.
Al momento della consegna, la videocamera è abbinata all'identificativo dell'operatore che la riceve, al fine di poter risalire, in caso di necessità, a chi ha effettuato le registrazioni.
E' dotata di un indicatore led che indica quando la registrazione è attiva.
A cessate esigenze, la videocamera viene inserita immediatamente nelle docking station.
Con l'inserimento nelle docking station i dati registrati dalle videocamere sono cancellati automaticamente e trasferiti nel NAS/PC del Reparto/Nucleo di Polizia Penitenziaria.
Il sistema body-cam è rappresentato in ***fig.1***; le componenti che costituiscono l'architettura della soluzione tecnologica devono essere costituite da:

1. Apparati di registrazione (body-cam);

Strumenti

Scheda di sintesi

Documenti

Domanda di partecipazione

2. Server centrale (metadati) presso Centrale Operativa Nazionale del Dipartimento dell'Amministrazione Penitenziaria (ubicata presso il Polo Logistico penitenziario di Roma "Rebibbia");
3. Totem multimediali presso i Reparti/Nuclei (ove sono alloggiati un personal computer, software di gestione, docking station per la ricarica delle videocamere e l'unità NAS per l'archiviazione dati);

FIG. 1

2.1. Risorse hardware, software e rete intranet\VPN ministeriale

L'architettura deve prevedere le seguenti componenti hardware.

Server centrale, così composto:

1. Dell EMC PowerEdge R450 con processori scalabili Intel Xeon di terza generazione comprensivo di 250 gb di memoria;
2. Avvio robusto con funzionalità di protezione della piattaforma, anche prima della creazione del server, tra cui la verifica dei componenti protetti e la Silicon Root of Trust
3. Dotato di intelligence, automazione e strumenti di ripristino che includono telemetria iDRAC9, scansione del BIOS in tempo reale e ripristino rapido del sistema operativo.

Presso gli Istituti penitenziari e gli Istituti penali per i minorenni sono distribuite:

1. Body-cam dotate di memoria non removibile;
2. Docking station per la ricarica dotati di porte USB 3.0;
3. Switch con porte rj45 10/100/1000 gigabit;
4. NAS equipaggiati con HD da 2,5 pollici da 2 TB con 128 mb di buffer;
5. Gruppo UPS.

Il Server centrale deve essere in grado di:

1. collezionare i dati relativi ai filmati registrati e conservati negli storage; interni ai PC dotati di software Client;
2. gestire le autorizzazioni di accesso ed i relativi profili utente;
3. gestire la distribuzione di aggiornamenti software e firmware per le camere;
4. gestione configurazione Server centrale (admin).

I PC dotati di software Client devono essere in grado di:

1. gestire la distribuzione delle policy di configurazione per le camere e per i PC dotati di software Client.

Lato Web (frontend), le principali funzionalità richieste sono:

1. login al sistema;
2. autenticazione e autorizzazione;
3. consultazione indice delle registrazioni;
4. consultazione metadati;
5. accesso ai contenuti autorizzati;
6. gestione configurazione camere (admin);
7. gestione configurazione PC (admin).

Le funzioni relative ai sottoelencati software devono essere accessibili unicamente dall'Amministratore del sistema:
Software - API, ospita i servizi (REST HTTPS) necessari al frontend e alla gestione delle funzioni applicative;

Software B2B, raggiungibile solo dal server API e utilizzato per lo scambio di informazioni con le altre componenti infrastrutturali già presenti nell'Amministrazione.
Software database Repository dei dati della soluzione, che comprendono:

1. informazioni per la profilazione degli utenti;
2. archivio metadati del materiale multimediale;
3. configurazioni applicative;
4. autorizzazioni e politiche di sicurezza;
5. chiavi di cifratura e hashing dei filmati.

Le componenti applicative che costituiscono la soluzione sono tre:

1. una componente installata sul PC, Client e Viewer;
2. una componente installata sul Server centrale;
3. un software di visualizzazione in grado di decifrare e mostrare i filmati Client.

Le principali funzionalità offerte dal *Client* installato presso i Reparti/Nuclei sono:

1. gestione dell'assegnazione/restituzione delle body-cam;
2. configurazione delle body-cam;
3. gestione dello scarico dei contenuti multimediali;
4. marcatura dei contenuti multimediali "rilevanti" ai fini investigativi;
5. gestione della cancellazione programmata dei filmati non marcati.

Software del Server centrale
L'accesso all'interfaccia offerta dal Server centrale è consentito all'Amministratore del sistema, al fine di:

1. gestire i profili degli utenti abilitati (admin);
2. gestire le configurazioni e le informazioni relative alle body-cam e alla configurazione del sistema (admin);
3. eseguire ricerche sui dati archiviati e relativi al materiale multimediale presente presso le postazioni Client.

Analogamente a quanto previsto per il *software* installato sulle postazioni *Client* e sulle *body-cam*, ogni operazione eseguita dagli utenti abilitati deve essere tracciata e registrata dal Server centrale.

Software Viewer
Tutti i filmati e i contenuti multimediali ripresi con le *body-cam* e raccolti nelle postazioni *Client* sono cifrati e possono essere visualizzati esclusivamente utilizzando il *software* installato sulle medesime postazioni, che è in grado di:

1. visualizzare i contenuti di un filmato cifrato;
2. verificarne la firma (hashing);
3. consentire il taglio del filmato (con creazione di una nuova copia di lavoro cifrata e firmata con hashing);
4. consentire l'esportazione del filmato decifrato con apposizione di marcatura in sovraimpressione ("copia per Autorità di Pubblica Sicurezza" o "copia per Autorità Giudiziaria").

2.2. Procedure tecniche di utilizzo del sistema
Al fine di garantire il corretto uso delle body-cam si individuano le seguenti procedure tecniche di utilizzo.
2.2.1. Censimento delle body-cam autorizzate
Il sistema deve prevedere che ogni body-cam sia censita, autorizzata, catalogata e

riconosciuta come dispositivo dal sistema stesso tramite un codice generato ad hoc all'atto della registrazione.
Questo codice, generato dal Server centrale, viene immagazzinato nella body-cam, che fornisce a sua volta una chiave al Server.
Lo scambio delle chiavi tra client e Server centrale garantisce il riconoscimento della body-cam come dispositivo appartenente al sistema e ne consente la corretta associazione al relativo Reparto/Nucleo.
La registrazione effettuata dalla body-cam sarà identificata con un codice che consente di risalire all'apparato che ha eseguito la ripresa.

2.2.2. Cifratura dei contenuti multimediali

I contenuti multimediali all'interno dello storage della body-cam sono cifrati con chiave AES a 128 bit e la chiave di decrittazione è cablata all'interno dell'applicativo.
Tutto il materiale multimediale non può essere quindi consultato direttamente dalla body-cam. Anche qualora si dovesse riuscire ad avere accesso ai contenuti, manomettendo la body-cam, non deve comunque essere possibile decifrarli per riprodurli.

2.2.3. Hashing (crittografia) del filmato

Questa funzionalità deve consentire che ogni volta che il filmato viene copiato o subisce una manipolazione venga generato un file hash contenente una firma, a sua volta generata tramite algoritmo SHA-256.
La prima firma viene generata non appena il filmato ripreso o la foto scattata dalla body-cam vengono consolidati sullo storage della body-cam stessa (cifrati).
Il file hash generato sulla body-cam viene poi trasferito, insieme al contenuto multimediale, sul NAS ed i suoi metadati vengono inviati al Server centrale.
Ogni successiva manipolazione del filmato, come l'applicazione della sovraimpressione per copia o il taglio del filmato, genera un nuovo file di contenuto ed un corrispondente file di hashing generato con lo stesso algoritmo e memorizzato sul NAS. I relativi metadati sono inviati al Server centrale.
Il riconoscimento degli utenti abilitati avviene tramite un sistema centralizzato di riconoscimento che si avvale di dominio intranet/VPN ministeriale.

2.2.4. Concatenamento dei tagli

E' richiesta questa funzionalità per consentire di identificare ed esportare la sola porzione di filmato veramente rilevante ai fini investigativi, senza esportare l'intero filmato, che potrebbe contenere altre informazioni non rilevanti e lesive del diritto alla privacy delle persone. Per garantire la possibilità di impedire eventuali manipolazioni successive all'esportazione del taglio, anche il nuovo contenuto multimediale generato viene firmato, generando il file di hash, e salvato sul NAS.
Le informazioni relative al taglio, incluso il contenuto del file hash, vengono salvate sul Server centrale e messe in relazione diretta con i filmati originali, in modo che sia sempre possibile risalire alla porzione del filmato originale da cui è stato eseguito il taglio, fino alla rimozione fisica del filmato dal NAS (che avviene per decorsi termini di conservazione). Anche dopo la cancellazione del filmato, le informazioni (metadati) salvate sul Server centrale restano registrate e consultabili, potendo quindi sempre risalire alle informazioni del filmato originale da cui è stato ricavato un taglio e ai relativi codici hash, da confrontare con quelli forniti insieme alla copia esportata.

2.2.5. Gerarchia di hashing

Ogni volta che si esporta o si manipola un contenuto multimediale, questo viene archiviato insieme ad un nuovo file di hash. Quando si esegue l'esportazione di un filmato, si esportano anche tutti i file di hash generati a partire dal file di hash originale generato sulla body-cam.
Questo consente di risalire, attraverso la consultazione del Server centrale all'intera gerarchia dei passaggi eseguiti per ottenere la copia del filmato, potendone quindi

certificare la conformità all'originale.
L'algoritmo per la generazione del file di hash è pubblico e riproducibile, così da consentirne l'esecuzione sulla copia in proprio possesso. L'esito dell'esecuzione dell'algoritmo di hashing sulla copia deve essere uguale al contenuto del file di hash corrispondente ai metadati inviati al Server centrale.

2.2.6. Imputabilità dei filmati (assegnazione e restituzione delle body cam)

Prima di consentire l'utilizzo di una body-cam, si richiede l'identificazione dell'operatore assegnatario tramite la digitazione di un codice. Questo codice viene quindi inviato alla body-cam prima di consentirne il prelievo dalla postazione locale.
Durante l'acquisizione del materiale multimediale, la body-cam imprime su ogni fotogramma alcune informazioni, tra le quali:

1. data e ora della ripresa. La sincronizzazione avviene con il server centrale durante il periodo di connessione al Totem;
2. codice associato al dispositivo, identificato all'atto della registrazione a sistema della camera;
3. codice dell'operatore assegnatario della camera.

Quando la camera viene restituita e inserita nella postazione locale, i contenuti multimediali registrati vengono automaticamente copiati sul NAS, le informazioni relative al filmato (metadati) sono inviate al Server centrale e la camera viene ripulita e re-inizializzata, rimuovendo il codice dell'operatore assegnatario. Ogni filmato ripreso è quindi imputabile all'operatore assegnatario della camera.

2.2.7. Protezione da riprese esterne (sovraimpressioni)

Ogni qual volta si utilizza il software di visione (viewer) per visualizzare un filmato, questo richiede l'autenticazione.
Il codice identificativo dell'operatore a cui era stata assegnata la body-cam viene visualizzato automaticamente durante la riproduzione del filmato, in posizione randomica e variabile ad intervalli di tempo casuali.
Questo accorgimento fa sì che, nel caso di ripresa del filmato in riproduzione con una videocamera esterna o con un cellulare, il filmato ripreso riporti sia il codice di colui che lo ha girato (impresso direttamente dalla body-cam) sia il codice dell'operatore che ne ha richiesto la visualizzazione.

2.2.8. Separazione tra i contenuti multimediali e le informazioni (metadati)

I contenuti multimediali acquisiti sono memorizzati localmente sulle postazioni locali, mentre le informazioni che descrivono il filmato, che includono anche l'evento a cui è associato e le note inserite dagli operatori, se disponibili, sono memorizzati sul Server centrale.
I dati sono, quindi, mantenuti separati e vengono ricongiunti solo quando gli operatori autorizzati ne eseguono richiesta, ricercando e visualizzando un filmato nell'indice centrale.
I log generati vengono mantenuti in locale e raccolti sul Server centrale ad ogni connessione.
L'accesso al filmato deve essere sempre tracciato e limitato alle sole funzionalità consentite dal sistema, come precedentemente illustrato.

2.3. Modalità di tracciamento delle operazioni

2.3.1. Server centrale

Gli accessi al sistema da parte degli operatori autorizzati generano un apposito file log nel Server centrale, contenente l'identificativo dell'operatore, l'orario di accesso, l'identificativo della macchina da cui è stato effettuato l'accesso sul NAS/PC, i dati ai quali si è acceduto e le operazioni compiute su tali dati.
Il file log non è modificabile e viene conservato in un database istituito nel Server centrale senza limitazioni temporali.

2.3.2. NAS/PC

Ogni volta che si esporta o si manipola un contenuto multimediale, questo viene archiviato insieme ad un nuovo file di hash. Quando si esegue l'esportazione di un filmato, si esportano anche tutti i file di hash generati a partire dal file di hash originale generato sulla camera. Questo consente di risalire, attraverso la consultazione del database del sistema centrale, all'intera gerarchia dei passaggi eseguiti per ottenere la copia del filmato, potendone quindi certificare la conformità all'originale. L'algoritmo per la generazione del file di hash è pubblico e riproducibile, così da consentirne l'esecuzione sulla copia in proprio possesso. L'esito dell'esecuzione dell'algoritmo di hashing sulla copia deve essere uguale al contenuto del file di hash corrispondente e alla copia salvata sul database del sistema centrale.

2.4. Protezione dai rischi informatici

Per quanto concerne le misure a protezione dei rischi informatici, le postazioni di lavoro verso il Server centrale devono essere protette tramite protocollo cifrato https.

Il contenuto delle videocamere è cifrato con chiave AES a 128 bit e la chiave di decrittazione è cablata all'interno dell'applicativo.

Il NAS deve prevedere la configurazione di due storage, logicamente separati:

1. uno storage, accessibile in lettura e scrittura, ma che non consenta la modifica delle informazioni registrate (ad eccezione della cancellazione sincronizzata con l'area di lavoro);
2. l'altro, utilizzato per memorizzare le copie di lavoro dei contenuti multimediali, che possono essere visionate con il viewer, manipolate ed esportate attraverso le funzionalità del sistema.

I contenuti del primo storage (golden copy) devono restare inalterati fino alla loro cancellazione e, qualora necessario, al fine di essere confrontati con le eventuali copie consegnate alle Autorità Giudiziaria a testimonianza della bontà della copia.
Si deve prevedere la creazione di copie di sicurezza a garanzia della salvaguardia dei dati oggetto di trattamento.
Per ogni NAS dovrà essere prevista una ridondanza di archiviazione, tramite un tool applicativo, che permetta di realizzare un backup cifrato dei file archiviati (con i relativi metadati), così da duplicare, automaticamente, il contenuto da una unità di archiviazione ad un'altra.
In tal modo si garantisce la disponibilità e la conservazione dei dati in caso di malfunzionamenti dell'unità di archiviazione primaria.

3. Procedimento di consultazione

Il procedimento di consultazione preliminare de quo si svolge nel rispetto degli articoli 66 e 67 del D.Lgs. n. 50/2016, nonché dei principi di non discriminazione e trasparenza, così come declinati nelle Linee guida n. 14 recanti "Indicazioni sulle consultazioni preliminari di mercato", approvate con delibera n. 161 del 6 marzo 2019 delle suddetta Autorità, a cui si rimanda integralmente, ed in particolare:

- i soggetti che partecipano alla consultazione forniscono consulenze, relazioni, dati, informazioni e altri documenti tecnici idonei a prestare il migliore apporto conoscitivo e informativo alla stazione appaltante procedente, relativamente all'individuazione del fabbisogno o delle soluzioni tecniche e/o organizzative idonee a soddisfare le esigenze funzionali indicate dalle stazioni appaltanti;
- i soggetti che partecipano alla consultazione indicano se i contributi forniti contengono informazioni, dati o documenti protetti da diritti di privativa o comunque rivelatori di segreti aziendali, commerciali o industriali, nonché ogni altra informazione utile a ricostruire la posizione del soggetto nel mercato e la competenza del soggetto nel campo di attività di cui alla consultazione.

4. Modalità di partecipazione

Gli operatori del mercato che ritengano di poter fornire il servizio in argomento dovranno far pervenire – **entro e non oltre le ore 14:00 dell'8 aprile 2023** - a mezzo PEC all'indirizzo ufficio2.dgrisorse.dap@giustiziacert.it, un elaborato, in formato .pdf, contenente una relazione tecnica, nonché eventuale ulteriore documentazione a corredo e quant'altro ritenuto utile a descrivere nel dettaglio la soluzione proposta, sottoscritto con firma digitale del legale rappresentante o da altro soggetto autorizzato, dal quale si dovranno evincere anche i dati dell'operatore economico con i relativi contatti.

La PEC dovrà riportare nell'oggetto la dicitura: "**Soluzioni tecnologiche per la ripresa di immagini per gli operatori di Polizia Penitenziaria impegnati in attività di servizio**"

Si precisa, altresì, che la presente consultazione di mercato non costituisce obbligo di procedere alle successive fasi di affidamento e, pertanto, non vincola in alcun modo l'Amministrazione penitenziaria verso gli operatori che presentino i propri elaborati, non trattandosi di avviso di gara o procedura di gara.

La valutazione in ordine alla scelta dello strumento contrattuale da adottare spetta esclusivamente all'Amministrazione.

Il presente avviso non costituisce un invito ad offrire né un'offerta al pubblico ai sensi dell'art. 1336 c.c. né una promessa al pubblico ai sensi dell'art. 1989 c.c.

La partecipazione alla presente consultazione non dà diritto a ricevere e/o a pretendere, a qualsiasi titolo, compensi e/o rimborsi e/o indennizzi di sorta.

L'Amministrazione si riserva di interrompere, sospendere o revocare la presente consultazione in qualsiasi momento, senza incorrere in alcun tipo di responsabilità.

I dati forniti dai soggetti proponenti verranno trattati, in conformità del Regolamento 2016/679/UE (GDPR), esclusivamente per le finalità connesse all'espletamento della presente consultazione. L'Amministrazione penitenziaria, salvo quanto di seguito previsto in materia di trattamento dei dati personali, si impegna a non divulgare a terzi le informazioni raccolte con la documentazione richiesta.

5. Richieste di chiarimenti

Eventuali richieste di chiarimenti relative agli aspetti tecnici della presente consultazione dovranno essere indirizzate a mezzo PEC all'indirizzo ufficio2.dgrisorse.dap@giustiziacert.it, indicando nell'oggetto "Richiesta chiarimenti - **"Soluzioni tecnologiche per la ripresa di immagini per gli operatori di Polizia Penitenziaria impegnati in attività di servizio"**

entro le ore 14:00 dell'1 aprile 2023.

Il referente amministrativo della procedura viene individuato nel Dirigente Aggiunto di Polizia Penitenziaria Massimo Milana - tel. 06.66591442; Peo massimo.milana@giustizia.it

Eventuali chiarimenti di carattere tecnico potranno essere richiesti al Funzionario Tecnico, Ing. Luigi Napolano (Peo luigi.napolano01@giustizia.it).

6. Pubblicazione avviso

Il presente avviso è pubblicato sul sito istituzionale www.giustizia.it del Ministero della Giustizia e sul sito www.serviziocontrattipubblici.it del Ministero delle Infrastrutture e della Mobilità Sostenibili.

Il Direttore generale reggente

Massimo Parisi