



Comune  
di Molinella

Città Metropolitana di Bologna

COMUNE DI MOLINELLA

# DATA PROTECTION IMPACT ASSESSMENT (DPIA)

## VALUTAZIONE D'IMPATTO

### BODYCAM

# DPIA

## Informazioni sulla PIA

Nome della PIA: Valutazione sull'utilizzo delle Bodycam

Nome autore dott. Giuliano Corso

Data di creazione 3.4.2025

Nome del DPO/RPD: Gloriamaria Paci  
Studio Paci  
Via Edelweiss Rodriguez Senior, 13 -  
47924 Rimini (RN)

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si ritiene opportuno procedere alla richiesta di alcun parere agli Interessati.

## Contesto

### Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento oggetto di valutazione, con la presente DPIA, riguarda:

- Trattamento di dati effettuato con strumenti di videosorveglianza, nello specifico registrazioni di vi-deo con la Bodycam. Si è proceduto all'acquisto complessivo di 4 Bodycam tipo Video Badge-440-64-KF-N, il cui utilizzo è finalizzato alla possibilità per gli agenti di indossarle sulla divisa nei servizi di controllo del territorio ai fini di tutela sia dell'agente in servizio che dei cittadini coinvolti. L'impiego di tali strumenti di acquisizione immagini è consentito solo se finalizzato alla prevenzione e/o accertamento di reati.

Quali sono i soggetti coinvolti e le responsabilità connesse al trattamento?

I soggetti coinvolti nell'attività di trattamento sono:

- a) il responsabile interno con qualifica di amministratore del sistema che potrà visionare le immagini registrate e disporre delle stesse;
- b) tutti gli operatori della Polizia Locale durante il servizio nel rispetto delle direttive fissate nel disciplinare tecnico;
- c) la società esterna che ha accesso ai dati (ad es. i manutentori, Sinora S.r.l.).

Ci sono standard applicabili al trattamento?

Attualmente non esistenti per la videosorveglianza.

# Dati, processi e risorse di supporto

## Quali sono i dati trattati?

I dati trattati consistono in immagini e video registrati sul piano operativo. La registrazione è attivata solamente dal personale incaricato qualora vi sia una situazione di particolare criticità che necessita la documentazione video degli eventi. Se attivata, la registrazione delle immagini avviene fino a 2 minuti precedenti e successivi all'attivazione.

## Qual è il ciclo di vita del trattamento dei dati?

Le videocamere sono contraddistinte da un numero seriale che dovrà essere annotato in apposito **registro**. L'amministratore del sistema è anche il responsabile della tenuta dei registri.

L'operatore di Polizia Locale attiverà il dispositivo, in relazione all'evolversi degli scenari che facciano presupporre criticità e provvederà a cessare le riprese al termine degli stessi. Le riprese potranno essere riattivate ogniqualvolta l'operatore stesso ne ravvisi la necessità.

I dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza per le finalità del vigente *"Regolamento per la disciplina della videosorveglianza nel territorio comunale di Molinella"*,
- conservati per un periodo di tempo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso per un periodo di tempo non superiore a sette giorni, fatte salve speciali esigenze di ulteriore conservazione. Al termine del tempo stabilito le riprese dovranno essere cancellate;
- trattati, con riferimento alla finalità rivolte a salvaguardare l'anonimato anche successivamente alla fase della raccolta, atteso che tali immagini registrate potrebbero contenere dati di carattere personale.

I trattamenti debbono rispettare i principi del Codice della Privacy; nello specifico deve essere eseguita una valutazione del rischio sul trattamento dei dati personali oggetto di trattamento, che debbono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato.

Il sistema di ripresa video con le microcamere dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza di concrete e reali situazioni di pericolo di turbamento dell'ordine e della sicurezza pubblica e per la tutela dell'incolumità fisica degli operatori e dei cittadini, nonché ai fini della tutela giuridica connessa ai procedimenti di specifico riferimento. In caso di registrazione di riprese in occasione di situazioni di presunto pericolo, come sopra meglio specificato, poi non concretizzatosi, le immagini stesse dovranno essere tempestivamente cancellate, in quanto il loro ulteriore trattamento risulterebbe estraneo alle finalità per cui sono impiegate.

**I video delle unità di ripresa, salvati su memoria interna, saranno scaricati tramite dispositivo locale presidiato su cloud riservato messo a disposizione dall'azienda SINORA Srl.**

Le immagini videoregistrate **sono conservate per un tempo non superiore a sette giorni**, fatte salve speciali esigenze di ulteriore conservazione nei limiti e con le modalità stabilite al punto 3.4. del provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010, ed in modo particolare, in relazione ad illecite che si siano verificati o ad indagini delle autorità giudiziaria o di pubblica sicurezza.

## Quali sono le risorse di supporto ai dati?

I dati delle prove vengono crittografati in transito e mentre sono a riposo in deposito. Sinora Srl mantiene procedure di gestione delle chiavi di crittografia mature e controllate.

Crittografia dei dati in transito:

FIPS 140-2 convalidato: Modulo crittografico AES-256. Implementazione TLS 1.2 con connessione a 256 bit, chiave RSA 2048 bit, Perfect Forward Secrecy Crittografia dei dati delle prove a riposo:

Conforme a CJIS, crittografia AES NSA Suite B a 256 bit

# Principi Fondamentali

## Proporzionalità e necessità

### Gli scopi del trattamento sono specifici, espliciti e legittimi?

La liceità è data dall'art. 6 par. 1 del GDPR, in quanto "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".

Il trattamento avviene altresì a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, ai sensi dell'art. 1 comma 2 del Dlgs 18 maggio 2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio".

La finalità di dotare gli operatori di una Bodycam persegue la sicurezza e l'incolumità dei collaboratori e/o dei cittadini, la tutela del patrimonio prevenendo e perseguendo il compimento di eventuali atti illeciti.

La ripresa dei video persegue altresì la tutela dell'ordine e della sicurezza pubblica, la prevenzione, l'accertamento e la repressione dei reati ed in particolare:

- l'attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale;
- la ricostruzione, in tempo reale, della dinamica di atti vandalici o fatti criminosi o azioni di teppismo nei luoghi pubblici di principale frequentazione, anche a tutela del patrimonio pubblico.
- in presenza di una specifica attività preventiva o repressiva di fatti di reato, situazioni dalle quali possano derivare minacce per l'ordine e la sicurezza pubblica o un pericolo per la vita e l'incolumità dell'operatore, o specifiche attività poste in essere durante il servizio che siano espressione di poteri autoritativi degli organi, uffici e comandi di polizia.

La possibilità di disporre in tempo reale di dati ed immagini costituisce un ulteriore strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell'ambito delle proprie competenze istituzionali sul territorio comunale in stretto raccordo con le altre Forze dell'Ordine; attraverso tali strumenti si persegue l'intento di tutelare la popolazione ed il patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.

Le microcamere – Bodycam e dashcam – **NON** potranno essere utilizzate, in base all'art. 4 dello Statuto dei lavoratori (legge n. 300 del 20 maggio 1970) per effettuare controlli sull'attività lavorativa dei dipendenti dell'Amministrazione comunale, di altre Amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

### Quali sono le basi legali che rendono lecito il trattamento?

Sulla base di quanto sopra indicato la liceità del trattamento è individuabile ex art. 6 par. 1 lett. E del GDPR, art. 5 del Dlgs 18 maggio 2018, n. 51 e art. 23, comma 1, del d.P.R. n. 15 del 2018.

### I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati vengono raccolti solo per l'attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale e per la ricostruzione, in tempo reale, della dinamica di atti vandalici o fatti criminosi o

azioni di teppismo nei luoghi pubblici di principale frequentazione, anche a tutela del patrimonio pubblico. Qualora la registrazione dei video risulti attivata e non ricorrano i presupposti sopra indicati si procederà immediatamente alla cancellazione dei dati.

### I dati sono esatti e aggiornati?

Non applicabile alla videosorveglianza tramite BodyCam.

### Qual è il periodo di conservazione dei dati?

Le immagini vengono registrate solo in presenza di un fatto che può costituire reato o nel contesto temporale e di luogo ove sono avvenuti altri fatti che possono costituire reato. Le registrazioni permangono in memoria fino all'esito giudiziale del procedimento correlato, altrimenti sono cancellati.

Sono ammessi tempi di conservazione superiori qualora si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o degli organi di polizia.

## Misure a tutela dei diritti degli interessati

### Come sono informati del trattamento gli interessati?

La bodycam presente sulla divisa è accompagnata dalla presenza di un'effigie visibile riportante l'immagine di una telecamera.

Gli agenti sono ad informare oralmente, qualora le circostanze lo permettano, dell'attivazione del sistema di telecamere.

Sul sito web istituzionale è pubblicata l'informativa completa di videosorveglianza, che copre tutte le attività di trattamento tramite strumenti di ripresa.

### Gli interessati sono messi in grado di esercitare i diritti di cui agli artt. 15 e seguenti?

In relazione al trattamento dei dati personali, è assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificarne le finalità, le modalità del trattamento e di ottenerne l'interruzione nel caso di utilizzo illecito, in particolare per la carenza dell'adozione delle idonee misure di sicurezza o per l'uso indebito da parte di soggetti non autorizzati.

I diritti di cui al presente articolo riferiti a dati personali concernenti persone decedute, possono essere esercitati dagli eredi, da chi abbia un interesse proprio, da chi agisca a tutela dell'interessato o per ragioni familiari considerate particolarmente meritevoli di protezione.

Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.

Nel caso di esito negativo alle istanze di cui al presente articolo, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

### Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

- Gli obblighi dei responsabili del trattamento sono determinati nel Disciplinare per l'utilizzo delle

- microcamere nei servizi a rischio operativo.
- La società Sinora Srl è stata nominata responsabile esterno (ai sensi dell'art. 28 GDPR) con apposito atto di nomina disponibile agli atti (Prot. n. 8769/2025).

I dati sono trasferiti al di fuori del territorio UE?

No.

## Rischi

### Indisponibilità dei dati (distruzione, perdita, furto)

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

In caso di indisponibilità dei dati non vi sarebbero particolari conseguenze per i diritti dei soggetti ripresi in quanto le immagini sono protette da crittografia. Inoltre, per visionare i dati contenuti il soggetto dovrebbe possedere una dock station.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

L'accesso illegittimo ai dati potrebbe occorrere o tramite accesso non autorizzato presso il Comando, ove si sottolinea è zona protetta e non accessibile al pubblico.

Altro accesso illegittimo potrebbe occorrere violando il server ove i dati sono protetti.

Non si ritiene un rischio il furto su strada delle Bodycam perché per visionare i dati contenuti il soggetto dovrebbe possedere una docking station per lo scarico dei dati.

Quali sono le fonti di rischio?

Si ritiene fonte di rischio l'accesso abusivo al Comando o l'accesso ai dati tramite la rete internet.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Per l'accesso al Comando di persone non dipendenti è permesso solo dopo l'identificazione e sono accolte da un dipendente del servizio cui accede.

La Motorola, produttrice delle bodycam, fornisce strumenti per limitare i rischi e garantire la sicurezza dei dati.

Molte delle funzionalità di controllo degli accessi possono essere abilitate o disabilitate dai clienti in base alle esigenze o possono essere modificate per soddisfare un livello specifico di rischio. Le impostazioni predefinite per queste funzionalità di sicurezza sono state scelte per fornire un forte livello di sicurezza, pur mantenendo flessibilità e praticità.

In merito all'autenticazione:

Lunghezza della password personalizzabile e requisiti complessi per le password Limite di accesso e durata di blocco non riusciti personalizzabili  
Impostazioni di timeout della sessione applicate  
Domande obbligatorie sulla sfida quando si autentica da nuove sedi  
Opzioni di autenticazione a più fattori per l'accesso dell'utente e prima delle azioni amministrative (codice una volta tramite SMS o telefonata)  
Limitare l'accesso a intervalli IP definiti (limitare l'accesso alle sedi di ufficio approvate)

In merito alle autorizzazioni:

Gestione granulare delle autorizzazioni basata sui ruoli  
Gestione delle autorizzazioni dell'applicazione (ad esempio, consentire a utenti specifici di utilizzare l'interfaccia basata sul Web,)  
Integrazione con i servizi directory per una gestione degli utenti semplificata e sicura

In merito al controllo e reporting e di gestione degli utenti:

Registrazione dettagliata delle attività dell'amministratore e dell'utente a prova di manomissione  
Portale Web di amministrazione intuitivo per gestire utenti, autorizzazioni e ruoli

In merito alla condivisione di dati:

Condivisione di prove all'interno dell'agenzia, tra agenzie ed esterne senza trasferimento di dati, duplicazione dei dati, supporti fisici o allegati e-mail.  
Registrazione dettagliata della catena di custodia durante la condivisione.  
Revocare l'accesso al contenuto condiviso in precedenza.  
Impedire a un destinatario di contenuto condiviso di scaricare o ricondividere le prove

Si richiamano altresì le misure normativo/disciplinari, fisiche, organizzative e logistiche descritte nel DISCIPLINARE PER L'UTILIZZO DEI SISTEMI DI RIPRESA VIDEO INDOSSABILI (BODYCAM) IN DOTAZIONE AL CORPO DI POLIZIA LOCALE DI MOLINELLA, allegato e parte integrante della presente DPIA

**Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure applicate/pianificate?**

Si ritiene il livello di rischio **Basso**.

**Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**

**Si ritiene la circostanza Improbabile.**

## **Integrità dei dati (alterazione, modifica)**

**Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?**

Qualora i dati fossero alterati o modificati non sarebbero producibili in giudizio e quindi nel procedimento penale sarebbe utilizzata la testimonianza dell'agente di Polizia Locale.

Si sottolinea che le registrazioni vengono crittografate evitando la possibilità di modificare le stesse.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Il sistema di sicurezza delle bodycam permette di evidenziare se tali accorgimenti sono stati violati segnalando la non conformità del video.

Per poter modificare i video le persone che si volessero cimentare dovrebbero possedere una tecnologia molto avanzata.

Quali sono le fonti di rischio?

Le fonti di rischio sono l'accesso ai server della Sinora Srl o l'accesso abusivo al Comando di Polizia Locale.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Per l'accesso al Comando i soggetti non appartenenti allo stesso si muovono all'interno solo accompagnati e durante la notte viene presidiato e attivato l'allarme a tutela dell'immobile.

Si richiamano altresì le misure normativo/disciplinari, fisiche, organizzative e logistiche descritte nel DISCIPLINARE PER L'UTILIZZO DEI SISTEMI DI RIPRESA VIDEO INDOSSABILI (BODYCAM) DEL COMUNE DI MOLINELLA, allegato e parte integrante della presente DPIA

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Il rischio viene valutato come **Basso**.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

La stima individua l'evento come **Improbabile**.

## **Riservatezza dei dati (accesso abusivo, trattamento non conforme)**

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

In caso di accesso illegittimo alle immagini si ritiene non si concretizzi un danno in quanto il soggetto prenderebbe semplicemente visione delle immagini registrate.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Accesso abusivo al server di Sinora Srl o accesso abusivo presso il Comando.

### Quali sono le fonti di rischio?

Accesso tramite internet o accesso abusivo fisicamente in Comando.

### Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Per l'accesso al Comando i soggetti non appartenenti allo stesso si muovono all'interno solo accompagnati e durante la notte viene presidiato e attivato l'allarme a tutela dell'immobile.

Si richiamano altresì le misure normativo/disciplinari, fisiche, organizzative e logistiche descritte nel DISCIPLINARE PER L'UTILIZZO DEI SISTEMI DI RIPRESA VIDEO INDOSSABILI (BODYCAM) E TELECAMERE A BORDO VEICOLO DI SERVIZIO (DASHCAM) IN DOTAZIONE AL CORPO DI POLIZIA LOCALE DI MOLINELLA, allegato e parte integrante della presente DPIA

### Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Il rischio viene valutato come **Basso**.

### Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

La stima individua l'evento come **Improbabile**.

## Piano d'azione

### Misure e Procedure adottate o programmate per la mitigazione dei rischi

I dati delle prove vengono crittografati in transito e mentre sono a riposo in deposito. Sinora Srl mantiene procedure di gestione delle chiavi di crittografia mature e controllate.

Crittografia dei dati in transito:

FIPS 140-2 convalidato: Modulo crittografico AES-256 Implementazione TLS 1.2 con connessione a 256 bit, chiave RSA 2048 bit, Perfect Forward Secrecy Crittografia dei dati delle prove a riposo:

Conforme a CJIS, crittografia AES NSA Suite B a 256 bit

#### Parere del DPO/RPD:

- a) Il disciplinare operativo body cam è accoglibile con le integrazioni di cui ai punti 1 e 2 (
- b) Per attivare le body cam, ai fini della conformità al Reg. UE n. 678/2016 nell'ordine è necessaria:
  - 1) Formalizzare la prima revisione della valutazione di impatto per l'utilizzo delle body cam.
  - 2) La sottoscrizione dell'accordo sindacale ex art. 4 c.1 della Legge n. 300/1970.
  - 3) Evidenza della nomina a responsabile del trattamento ex art. 28 del Regolamento (UE) 2016/679 sottoscritta tra il Comune di Molinella e Sinora S.r.l. per tale specifico trattamento dati
  - 4) L'informativa completa da pubblicare sul sito rivolta ai soggetti interessati ripresi.

## Data Protection Impact Assessment (DPIA) Impianto di Videosorveglianza Comunale

---

- 5) L' informativa completa da predisporre per gli agenti della Polizia Locale si ricorda che i soggetti interessati al trattamento dati per effetto dell' utilizzo delle body cam sono sia i cittadini ripresi che i dipendenti del comune quali agenti della P.L.
- 6) Le designazioni dei soggetti autorizzati e la almeno la programmazione della formazione degli operatori che utilizzeranno il sistema, se non già svolta.
- 7) Procedere con la predisposizione degli aggiornamenti in adempimento del Reg. UE 2016/679 riguardo al registro del trattamento

Allegato 1: DISCIPLINARE PER L'UTILIZZO DEI SISTEMI DI RIPRESA VIDEO INDOSSABILI (BODYCAM) E TELECAMERE A BORDO VEICOLO DI SERVIZIO (DASHCAM) IN DOTAZIONE AL CORPO DI POLIZIA LOCALE DI MOLINELLA

Il Comandante

Dott. Giuliano Corso

(documento firmato digitalmente)