Provvedimento del 4 dicembre 2025 [10221993]

VEDI ANCHE Newsletter del 20 febbraio 2026

[doc. web n. 10221993]

Provvedimento del 4 dicembre 2025

Registro dei provvedimenti
n. 743 del 4 dicembre 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla presenza del professor Pasquale Stanzione, presidente, della professoressa Ginevra Cerrina Feroni, vicepresidente, dell'avvocato Guido Scorza e del dottor Agostino Ghiglia, componenti e del dottor Luigi Montuori, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati, di seguito anche "Regolamento");

VISTO il decreto legislativo 30 giugno 2003, n.196, recante il Codice in materia di protezione dei dati personali, integrato con le modifiche introdotte dal decreto legislativo 10 agosto 2018, n. 101 (di seguito anche: "Codice");

VISTA la 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;

VISTO il decreto legislativo 18 maggio 2018, n. 51, recante l'Attuazione della direttiva (UE) 2016/680 (di seguito anche "Decreto");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali (di seguito: "Regolamento 1/2019");

ESAMINATA la valutazione di impatto sulla protezione dei dati personali (Data Protection Impact Assesment, di seguito anche "DPIA") del sistema videocamere operative individuali (body cam) da fornire in dotazione agli agenti della Polizia Locale del Comune di Pescara;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale, ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell´ufficio del Garante per la protezione dei dati personali;

Relatore professoressa Ginevra Cerrina Feroni;

PREMESSO

1. Il Comune di Pescara ha inviato a questa Autorità una DPIA relativa ad un sistema videocamere operative individuali (body cam) da fornire in dotazione agli agenti della Polizia locale ed un Disciplinare per l'uso delle videocamere operative individuali (breviter Disciplinare), chiedendo a questa Autorità di effettuarne una valutazione preventiva.

Occorre premettere che tale DPIA costituisce una quarta versione emendata delle precedenti, estremamente carenti, del 18 ottobre 2022, per la quale l'Ufficio del Garante inviò al Comune la nota di osservazioni del 27 febbraio, dell'11 agosto 2023, per la quale l'Ufficio del Garante inviò al Comune la nota di osservazioni dell'8 novembre 2023 e del 18 giugno 2024, per la quale l'Ufficio del Garante inviò al Comune la nota di osservazioni del 24 settembre 2024.

La quarta versione della DPIA, oggetto dell'attuale provvedimento, inviata il 12 giugno 2025, sarebbe stata redatta dal Comune "in accoglimento dei suggerimenti forniti con la nota in riferimento", ossia la precitata nota del 24 settembre 2024.

2. Soggetti coinvolti nel trattamento dei dati.

Il Titolare del trattamento è il Comune di Pescara, nella persona del legale rappresentante del Sindaco p.t.; il soggetto autorizzato al trattamento è il Comandante del Corpo di Polizia locale di Pescara, autorizzato con delega (SATD) dal Sindaco; autorizzati al trattamento e quindi autorizzati ad utilizzare le telecamere portatili (body cam), nei casi in cui sia indispensabile per gli scopi perseguiti, sono i soggetti in servizio presso il Corpo di Polizia locale di Pescara, specificamente designati con provvedimento del Comandante del Corpo; i soggetti autorizzati a visionare le immagini registrate dai predetti dispositivi sono diversi da coloro che hanno acquisito e riversato le immagini in ripresa; il responsabile del trattamento è fornitore del servizio cloud, con cui viene sottoscritto un contratto disciplinante gli obblighi in materia di protezione dei dati personali.

3. Scopo, finalità del trattamento e scenari di utilizzo.

La DPIA prevede di dotare personale della Polizia locale di body cam da impiegare per finalità di acquisizione di prova, nell'ambito dello svolgimento delle attività ausiliarie di pubblica sicurezza esercitate ai sensi dell'articolo 3 della legge n. 65/1986, della vigilanza e prevenzione reati e dell'attività di polizia giudiziaria.

In particolare, l'impiego delle body cam è previsto in una delle seguenti circostanze:

a. in luoghi pubblici o aperti al pubblico, al compimento delle "attività di pubblica sicurezza", senza alcuna possibilità di utilizzare il sistema per l'acquisizione e utilizzo delle registrazioni in funzione probatoria dell'accertamento di illeciti amministrativi;

b. in luoghi pubblici o aperti al pubblico nonché in luoghi privati, al compimento delle "attività di polizia giudiziaria" (es. arresto d'iniziativa in flagranza di reato, resistenza e fuga del sospettato di reato, perquisizioni e sequestri d'iniziativa o delegati, esecuzione di misura cautelare delegata dall'A.G., altre circostanze legittimanti l'uso di mezzi di coazione fisica), per la possibile acquisizione delle registrazioni quale indizio o fonte di prova dell'eventuale reato tentato o consumato;

c. in tutte le situazioni di ipotetica insorgenza di tangibili situazioni di pericolo, di turbamento dell'ordine e della sicurezza pubblica;

d. in caso di pericolo imminente per persone e/o cose o di insorgenza di situazioni di criticità che legittimino l'operazione di acquisizione, ivi compresa l'incolumità dell'operatore di Polizia locale.

Le immagini potranno essere utilizzate come fonti di prova anche per l'esercizio del diritto di difesa dell'operatore di Polizia locale in caso di contestazione del suo operato, nonché di esercizio del diritto di difesa delle persone vittime di reato.

L'operatore interromperà la registrazione quando non dovessero più sussistere le circostanze che hanno portano ad attivarla.

Le immagini, laddove rappresentative di fatti costituenti reato, sono immediatamente messe a disposizione dell'Autorità Giudiziaria e non possono essere conservate dal Comune, salvo autorizzazione del Giudice e limitatamente a favore dei Corpi della polizia locale operanti in qualità di agenti di polizia giudiziaria.

4. Liceità e base giuridica del trattamento.

Nella DPIA sono indicate come condizioni di liceità del trattamento l'articolo 6, par. 1, del Regolamento, 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", nonché l'articolo 1, comma 2, del D.lgs. 18 maggio 2018, n. 51, essendo il trattamento effettuato ai 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.

Per quanto riguarda le fonti giuridiche di legittimazione del trattamento, la DPIA richiama il decreto-legge n. 14/2017 (Disposizioni urgenti in materia di sicurezza delle città), nella parte in cui prevede che le polizie locali sono chiamate ad intervenire e collaborare con le Forze di Polizia al fine di tutelare l'incolumità pubblica, l'integrità fisica della popolazione, la sicurezza urbana, prevenire e contrastare l'insorgere di fenomeni criminosi o di illegalità, quali lo spaccio di stupefacenti, lo sfruttamento della prostituzione, la tratta di persone, l'accattonaggio con impiego di minori e disabili, o di violenza, anche legati all'abuso di alcool o all'uso di sostanze stupefacenti.

Sono, altresì, richiamate le disposizioni del codice di procedura penale in materia di acquisizione di materiale probatorio da parte della polizia giudiziaria (artt. 55 e 234 c.p.p.), l'articolo 10, comma 6-quater, del citato d.l. n. 14/2017, con riferimento alla flagranza differita ed infine il d.P.R. 15 gennaio 2018, n. 15, recante il regolamento, a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per finalità di polizia, da organi, uffici e comandi di polizia.

5. Dati personali oggetto del trattamento.

I dati trattati consistono in immagini e video registrati sul piano operativo; sono, inoltre, archiviati i dati relativi alla data, all'ora e al GPS, sempre per le finalità descritte.

Non verranno utilizzati dispositivi tecnici diretti a consentire l'identificazione univoca o l'autenticazione di una persona fisica (facial recognition).

6. Autorizzati al trattamento e procedure di assegnazione e consegna delle body cam.

È previsto il conferimento per iscritto dell'autorizzazione al trattamento dei dati personali, con informazione sui relativi poteri in capo a ciascuna categoria di operatore.

Le body cam sono assegnate agli operatori individuati dal Comandante del Corpo di Polizia locale tramite ordine di servizio; al momento della consegna e riconsegna v'è annotazione su apposito registro. Al momento della riconsegna del dispositivo si deve comunicare se sono state effettuate registrazioni. Si precisa che, per la stessa natura dei dispositivi, l'operatore non può effettuare operazioni di modifica, cancellazione o duplicazione delle immagini raccolte. Si precisa, inoltre,

che le body cam sono consegnate agli operatori prive di ogni dato registrato.

E' previsto un Registro delle assegnazioni delle body cam in formato cartaceo, con pagine numerate e sottoscritte dal Comandante del Corpo di Polizia locale. Dovranno registrarsi giornalmente i dati degli assegnatari e dei rispettivi strumenti affidati, il giorno e l'ora di affidamento, il giorno e l'ora di riconsegna, con una casella dedicata all'indicazione relativa alla presenza o meno di registrazioni. Al fine di tutelare la riservatezza dell'operatore, quest'ultimo sarà identificato con un codice noto solo a questi, al Comandante e al responsabile del servizio di visione delle videoregistrazioni.

Maggiori dettagli sono contenuti nell'allegato Disciplinare per l'uso delle body cam.

7. Modalità e durata della conservazione delle immagini.

I dati personali acquisiti vengono conservati tramite download su cloud certificato e qualificato AGID fornito da responsabile esterno. *[OMISSIS]* È possibile la generazione di log che certificano tutte le attività effettuate su una specifica prova, riportando informazioni quali: data/ora/Utente loggato/Ip della macchina da cui è stato effettuato l'accesso e l'azione effettuata sulla prova. Il sistema conserverà i dati relativi alle operazioni di cancellazione dei dati effettuate dagli operatori autorizzati alla visione.

Quanto ai tempi di conservazione dei dati, è prevista la loro cancellazione entro le ventiquattro ore ove non vi siano immagini relative a reati. In caso di ripresa di reati, il termine di cancellazione è di sette giorni e, comunque, i dati non verranno conservati (e per l'effetto verranno cancellati) una volta conferiti all'Autorità giudiziaria, salvo che quest'ultima ne disponga la conservazione.

Il software della società fornitrice consente di programmare la cancellazione dei files raccolti, con la definizione di un tempo prestabilito di mantenimento dei filmati esprimibile in giorni/mesi/anni.

Le registrazioni avviate accidentalmente, in mancanza del requisito della necessità o avviate in previsione dell'insorgenza di situazioni "critiche" che non si siano poi verificate, sono cancellate tempestivamente dagli addetti alla visione delle registrazioni a seguito della formale comunicazione dell'agente che li abbia colti. E' fatto obbligo agli agenti di segnalare al momento della riconsegna delle body cam eventuali registrazioni accidentali azionate.

8. Informativa agli interessati.

Sarà pubblicata un'informativa sul sito istituzionale della Polizia locale (poliziamunicipale.comune.pescara.it) e, laddove sia compatibilmente possibile con gli eventi, sarà resa informazione orale dell'attivazione della body cam da parte dell'operatore.

9. Misure di sicurezza.

[OMISSIS] non è previsto il trasferimento dei dati personali trattati al di fuori della UE, *[OMISSIS]*.

10. Valutazione dei rischi

L'ultima parte della DPIA è dedicata alla valutazione dei rischi per gli interessati, con riferimento ai rischi di accesso illegittimo ai dati, di modifiche indesiderate e di perdita di dati. All'esito delle misure adottate, la DPIA valuta la probabilità del rischio residuo limitata.

CONSIDERATO

11. Come premesso, la DPIA costituisce una quarta versione di precedenti, ciascuna delle quali presentava gravi lacune che sono state evidenziate al Comune con dettagliate note di

osservazioni, anch'esse sopra richiamate.

Con l'ultima nota di osservazioni si rilevava la permanenza, nella versione inviata il 17 giugno 2024, di alcune incongruenze – ancorché segnalate in precedenza - di seguito specificate:

11.1 Nei testi trasmessi permanevano indicazioni contraddittorie in merito al quadro giuridico di riferimento in quanto, nonostante che il trattamento in esame rientrasse unicamente nel campo di applicazione del Decreto, perduravano riferimenti al Regolamento, con conseguente ambiguità sull'aspetto fondamentale delle effettive finalità del trattamento e della relativa disciplina applicabile in materia di protezione dei dati personali, compresa la stessa modalità di valutazione della DPIA. Sempre in merito alle fonti di riferimento, nel precedente riscontro di questa Autorità veniva segnalato che il d.P.R. 15 gennaio 2018, n. 15, richiamato nella DPIA, non si applica ai soggetti pubblici che, pur effettuando il trattamento dei dati personali per finalità di polizia, non rientrano nella categoria degli organi, uffici e comandi di cui all'articolo 57 del d. lgs. 30 giugno 2003, n. 196, onde gli organi della Polizia municipale sono esclusi dall'applicazione del predetto regolamento. Tuttavia, tale riferimento era stato mantenuto (pag. 6 della DPIA), senza alcuna motivazione al riguardo.

11.2 La DPIA prevedeva che le registrazioni di riprese in occasione di situazioni di presunto pericolo, poi non concretizzatosi, sarebbero state cancellate entro 24 ore, ma facevano salvi possibili rinvii dell'operazione di cancellazione al primo giorno utile, in caso di "specifici impedimenti organizzativi dettati da turnazioni, festività o chiusura di uffici o esercizi", previsione peraltro mai riscontrata nelle DPIA sull'impiego delle bodycam, sia in ambito nazionale che locale, che il Garante ha esaminato. In merito, si osservava che l'organizzazione deputata alla gestione del sistema in argomento dovrebbe essere strutturata in modo da evitare ritardi nelle operazioni necessarie per il corretto trattamento dei dati personali, limitando le ipotesi di ritardi ad eventi realmente eccezionali ed imprevedibili, quali non appaiono essere le turnazioni, le festività o la chiusura programmata di uffici ed esercizi.

11.3 Circa i file log, compresi quelli relativi alle operazioni di cancellazione dei dati, il paragrafo della DPIA intitolato "Tracciabilità" ne prevedeva correttamente la conservazione, ma non ne indicava la durata, da specificare con termine certo.

11.4 Per quanto riguarda la valutazione dei rischi, si rilevava una individuazione approssimativa dei rischi e delle conseguenze che potrebbero derivare dal trattamento per i diritti e le libertà degli interessati, aspetto che costituisce l'oggetto principale della DPIA.

11.5 Altre gravi lacune riguardavano le modalità di conservazione dei dati, poiché mentre la DPIA prevedeva che il download dei dati venisse effettuato su cloud fornito dal responsabile esterno del trattamento (pag. 3), il Disciplinare (art. 8, pag. 5) prevedeva che "le immagini scaricate dalle bodycam verranno conservate, ove possibile, in cartelle predisposte su server dedicato dell'amministrazione comunale o su piattaforma cloud certificata, ad accesso riservato, tramite sistemi protetti da password individuali a cui potranno accedere solo soggetti preventivamente autorizzati.". In merito, si rilevava che la scelta sulla modalità di conservazione dei dati doveva precedere la valutazione di impatto, in quanto questa deve indicare specificamente le caratteristiche di sicurezza logica e, ove occorra, fisica, del sistema predeterminato per lo storage dei dati personali. Circa l'eventuale uso di un server dedicato dell'Amministrazione comunale, il Disciplinare illustrava la politica in termini del tutto generici ed insufficienti, limitandosi ad indicare che l'accesso sarebbe riservato "tramite sistemi protetti da password individuali a cui potranno accedere solo soggetti preventivamente autorizzati". In ordine al sistema in cloud, sebbene la valutazione di impatto riportasse alcune informazioni sulla sicurezza del sistema, esse erano parziali, non completamente comprensibili o apparentemente risalenti (ad esempio, il protocollo SSL, indicato nella DPIA, è considerato obsoleto dal 2015).

Pertanto, per consentire a questa Autorità una valutazione compiuta del sistema in argomento, anche considerando che tale sistema sarebbe utilizzato per la realizzazione di un trattamento ad elevato rischio, si richiedeva di fornire le seguenti documentazioni e informazioni:

- copia della documentazione tecnica rilasciata dal produttore recante, con un adeguato livello di approfondimento, le caratteristiche tecniche del sistema, con particolare riferimento a:

  a. l'architettura del sistema informatico, il dettaglio delle componenti software, dei protocolli di trasferimento dei flussi dati e degli algoritmi di sicurezza;

  b. le specifiche tecniche delle videocamere scelte dal Comune e le misure di sicurezza idonee a garantire che l'estrazione dei dati acquisiti sia possibile solo ad opera di soggetti abilitati e verso il sistema informatico autorizzato;

  c. l'eventuale esistenza di una componente client cui è collegata la "rastrelliera" per lo stazionamento delle videocamere;

  d. le ragioni per la presenza di "sim" nelle videocamere;

  e. la descrizione in dettaglio delle modalità di cifratura dei dati, tra cui le politiche di gestione delle chiavi crittografiche per la cifratura dei dati quando memorizzati nelle memorie delle videocamere. Era necessario chiarire, inoltre, se le chiavi per la cifratura dei dati nelle memorie delle videocamere e quelle per la cifratura dei dati nel cloud (cifratura at rest), fossero nell'esclusiva disponibilità del titolare del trattamento o se ne fosse a conoscenza anche il produttore o il fornitore della soluzione software in adozione;

  f. la descrizione in dettaglio delle modalità di autenticazione che è possibile configurare per l'accesso al sistema, specificando se è possibile abilitare l'autenticazione multifattoriale, e se fosse possibile l'integrazione della procedura di autenticazione con il dominio di sicurezza dell'amministrazione (ad esempio, Active Directory di Microsoft);

  g. dettagli sulla postazione o sulle postazioni client utilizzate per il trattamento;

  h. dettagli sulle modalità con cui sono realizzati i backup dei dati;

  i. se fosse consentito l'accesso al sistema informatico dall'esterno dei locali dell'amministrazione: in tal caso, fornendo dettagli sulle modalità di accesso e sulle caratteristiche tecniche del collegamento VPN adoperato;

  j. dettagli sui meccanismi adoperati per garantire l'integrità dei dati durante tutte le fasi del trattamento;

- copia della bozza di contratto di acquisto del sistema informatico riportante, tra l'altro, l'ubicazione dei sistemi cloud utilizzati;

- chiarimenti sulle modalità tecniche adoperate per la trasmissione, quando previsto, delle immagini e dei filmati agli "organi di Polizia Giudiziaria" e agli "organi di Pubblica sicurezza".

RITENUTO

12. Ancorché l'ultima versione della DPIA accolga alcuni dei rilievi formulati dall'Ufficio del Garante, permangono numerose e rilevanti criticità di seguito indicate, nonostante siano state più volte segnalate al Comune nelle precedenti interlocuzioni.

12.1 Permangono nella DPIA riferimenti, quali fonti di legittimazione del trattamento, sia al Regolamento (pagg. 6 e 7), sia al d.P.R. 15 gennaio 2018, n. 15 (pag. 7), oltre che correttamente al Decreto, indicandosi che “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.”.

12..2 Non è stata tuttora indicata la durata della conservazione dei file di log.

12.3 E’ confermata la presenza di sim all’interno delle body cam ma non sono stati forniti i chiarimenti richiesti sui motivi di tale presenza.

12.4 Per quanto riguarda la sicurezza delle soluzioni tecnologiche scelte, le modifiche apportate all’ultima versione della DPIA sono minimali e non forniscono risposta alcuna alle richieste di approfondimento tecnico formulate dall’Ufficio del Garante.

In particolare, posto che il sistema di body cam si avvale per la gestione dei dati del prodotto XX di (XX), azienda statunitense, il Comune non ha chiarito né documentato se la scelta dello specifico prodotto sia scaturita da una valutazione comparativa con altre soluzioni presenti nel mercato e in che modo tale scelta abbia tenuto conto degli aspetti di protezione dei dati personali connessi alla natura ad elevato rischio del trattamento.

Il sistema informatico di XX con cui il titolare intende strutturare il proprio trattamento è dotato di certificazioni tecniche ed è censito nel catalogo dei servizi cloud dell’Autorità per la cybersicurezza nazionale come servizio SaaS con qualificazione di livello 2, elementi, questi, che certamente concorrono ad aumentare la fiducia sulla robustezza del sistema nei confronti di eventuali attacchi esterni provenienti da cybercriminali (pur non essendo stata resa disponibile documentazione tecnica di dettaglio consultabile).

Tuttavia, si rileva che il sistema di XX è completamente in cloud: sebbene il produttore dichiari di adoperare tecniche crittografiche sui dati a riposo e durante la trasmissione (v. XX), sinteticamente citate anche dal Comune di Pescara nella propria DPIA, non sono disponibili sufficienti dettagli tecnici sul processo di gestione delle chiavi crittografiche che consentano di escludere la possibilità che il fornitore del servizio possa accedere ai dati del titolare in chiaro.

La possibilità di accesso remoto a tali sistemi di trattamento ed ai dati ivi contenuti da parte di soggetti stabiliti al di fuori dell’Unione Europea configurerebbe, ove non escluso, un trasferimento di dati verso Paesi terzi, in violazione di quanto disposto dall’articolo 31, comma 1, lettera b) del Decreto, secondo cui, nell’ambito dei trattamenti rientranti nel capo di applicazione della Direttiva, i dati personali possono essere trasferiti ad un soggetto in un Paese terzo o a un'organizzazione internazionale che sia un'autorità competente per le finalità di law enforcement, competenza non ascrivibile ad XX.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell’articolo 24, comma 5, del decreto legislativo 18 maggio 2018, n. 51, esprime parere non favorevole in ordine alla valutazione di impatto sulla protezione dei dati personali, presentata dal Comune di Pescara, relativa ad un sistema videocamere operative individuali (body cam) da fornire in dotazione agli agenti della Polizia locale.

Roma, 4 dicembre 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Montuori