Provvedimento dell'11 giugno 2026 [10277202]

[doc. web n. 10277202]

Provvedimento dell'11 giugno 2026

Registro dei provvedimenti
n. 425 dell'11 giugno 2026

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla presenza del professor Pasquale Stanzione, presidente, della professoressa Ginevra Cerrina Feroni, vicepresidente, del dottor Agostino Ghiglia, componente 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”) relativa all’utilizzo dei dispositivi “bodycam” da parte degli agenti di Polizia locale del Comune di Brescia;

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 il dottor Agostino Ghiglia;

PREMESSO

1. Il Comune di Brescia ha inviato a questa Autorità una DPIA relativa ad un sistema di videocamere operative individuali (body cam) da fornire in dotazione agli agenti della Polizia locale.

Occorre premettere che tale DPIA costituisce una nuova versione emendata di una precedente, in relazione alla quale l'Ufficio del Garante inviò al Comune la nota di osservazioni del 10 giugno 2025 prot. U.0082938 per rilevare importanti criticità del testo, concernenti l'indicazione della base giuridica del trattamento, insufficiente previsione di misure a tutela dei diritti e libertà dei dipendenti del Comune coinvolti nel trattamento - anche in considerazione delle vigenti disposizioni in materia di controllo a distanza dell'attività dei lavoratori - mancata indicazione della specifica durata della conservazione dei file di log, erronea valutazione del trattamento come non effettuato su larga scala, eventuale sussistenza di funzioni di intelligenza artificiale, nonché la mancanza di informazioni su importanti dettagli tecnici, quali le regole di formazione e gestione delle chiavi crittografiche, modalità di autenticazione per l'accesso al sistema e abilitazione dell'autenticazione multifattoriale, l'ubicazione dei sistemi cloud utilizzati, la possibilità di accesso al sistema informatico dall'esterno dei locali dell'amministrazione.

La nuova versione della DPIA, oggetto dell'attuale provvedimento, datata 22 settembre 2025, è stata redatta dal Comune in dichiarata "conformità alle indicazioni fornite" con la predetta nota dell'Ufficio del Garante.

2. Finalità del trattamento.

Il trattamento descritto nella DPIA riguarda l'uso delle body cam da parte degli agenti del Corpo di Polizia locale di Brescia nel corso di eventi che richiedono l'esercizio di funzioni di polizia giudiziaria; la finalità specifica del trattamento di dati connesso all'impiego di body cam consiste nel raccogliere e conservare elementi di prova audio-video o fotografici riguardanti condotte illecite, rilevanti sotto l'aspetto penale, nonché per l'applicazione di altre misure contemplate dal sistema penale.

3. Base giuridica del trattamento.

La base giuridica che legittima il trattamento in argomento è costituita nell'articolo 5, primo comma, lett. a), della legge 7 marzo 1986, n. 65, che assegna al personale che svolge servizio di polizia municipale, nell'ambito territoriale dell'ente di appartenenza e nei limiti delle proprie attribuzioni, le funzioni di polizia giudiziaria, rivestendo a tal fine la qualità di agente di polizia giudiziaria, riferita agli operatori, o di ufficiale di polizia giudiziaria, riferita ai responsabili del servizio o del Corpo e agli addetti al coordinamento e al controllo. Analoga fattispecie è altresì prevista dall'articolo 57 del D.P.R. 22 settembre 1988, n. 447 (c.d. Codice di procedura penale).

4. Soggetti coinvolti nel trattamento dei dati.

Titolare del trattamento è il Comune di Brescia. Il Comandante pro-tempore del Corpo di Polizia locale è individuato quale designato dal titolare.

La società XX che fornisce la piattaforma cloud nella quale sono archiviate le immagini riprese con le body cam, è nominata responsabile del trattamento con apposito atto di nomina, depositato in atti (allegato 0.6).

L'impiego delle body cam è riservato agli operatori di Polizia locale debitamente autorizzati dal titolare; questi sono formati con sessioni teorico-pratiche sull'utilizzo dei dispositivi e mediante emanazione di regole scritte (disciplinare operativo di istruzione per l'impiego di sistemi di videosorveglianza indossabile in attuazione dell'articolo 16 del Regolamento per la disciplina dei sistemi di videosorveglianza comunale adottato con delibera del Consiglio Comunale in data 29.03.2023 n.24, depositata in atti).

I predetti, lavoratori dipendenti del Comune, rientrano anche tra i soggetti qualificabili come interessati. I diritti per una loro eventuale implicazione nei procedimenti di ripresa sono pienamente tutelati dall'articolo 10 del d. lgs. 51/2018. Infatti, rientra tra le competenze dell'agente assumere un ruolo che comporta la possibilità di essere ripreso, nell'ambito di un eventuale procedimento penale. Non si tratta di un trattamento sistematico e generalizzato, bensì di un trattamento contestualizzato al singolo evento o intervento, in cui l'agente, per la funzione esercitata, si assume anche le relative responsabilità connesse all'eventuale procedimento penale che ne possa derivare e quindi all'utilizzo della ripresa video. Essi sono destinatari di una apposita informativa, distinta da quella prevista per i soggetti esterni interessati dalle riprese video. E' stato inoltre stipulato un accordo sindacale, ai sensi dell'articolo 4 della legge n. 300 del 1970 (Statuto dei lavoratori), depositato in atti.

Quanto agli interessati "esterni", cioè i soggetti ripresi dalle body cam identificati o identificabili, il regolamento comunale sulla videosorveglianza, depositato in atti, assicura loro 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.

Oltre all'informativa estesa prevista dall'articolo 10 del d. lgs. 51/2018, da diffondere attraverso pubblicazione sul sito istituzionale del Comune di Brescia (depositata in atti), l'impiego dei dispositivi di videosorveglianza mobile viene segnalato con informazione "minima", attuata con le seguenti modalità:

- il dispositivo deve essere indossato dall'operatore di Polizia locale assegnatario in modo non occulto e conformemente con la foggia dell'uniforme indossata; [OMISSIS]

- in caso di avvio delle riprese audio e video, l'operatore dovrà avvisare i presenti – in modo da essere udibile e comprensibile – dell'attivazione del dispositivo e che i filmati saranno conservati per l'eventuale accertamento di reati ed eventualmente messi a disposizione dell'Autorità giudiziaria;

- in ogni caso, all'attivazione della registrazione dell'evento, l'operatività deve essere segnalata dalla presenza di led rossi lampeggianti.

5. Modalità di impiego e scenari di utilizzo.

Gli operatori assegnatari vengono individuati, secondo ragioni di opportunità e di effettiva esigenza di servizio, con provvedimento del Comandante del Corpo della Polizia locale.

Il dispositivo (identificato da numero di serie apposto sullo stesso o da numerazione univoca), corredato dai relativi accessori, per il tempo di utilizzo in servizio è considerato dotazione individuale degli assegnatari, che saranno ritenuti responsabili dell'eventuale incuria, danneggiamento e/o uso improprio.

L'assegnazione del dispositivo avviene mediante accesso a specifico armadio, apribile previo riconoscimento *[OMISSIS]* e compilazione obbligatoria di apposito registro appositamente custodito *[OMISSIS].*

L'attivazione dei dispositivi tipo body cam avviene di norma su ordine dell'Ufficiale, presente, più alto in grado. Nei casi di particolare necessità ed urgenza, nonché in assenza di un Ufficiale, potrà avvenire a cura dell'operatore assegnatario, qualora in situazioni direttamente connesse all'attività istituzionale, si verifichi una delle seguenti situazioni:

a) tutela dell'incolumità dell'operatore, in presenza di concreto pericolo conseguente ad

aggressioni o altre situazioni di conflitto;

b) assicurazione delle fonti di prova ex art. 348 c.p.p.;

c) indagini di polizia giudiziaria che richiedano l'esecuzione di accertamenti e rilievi ex art. 354 c.p.p.;

d) nella flagranza di reato o comunque di concreto pericolo di danno a persone e cose, desumibile dalle circostanze.

Nei casi sopra indicati, all'attivazione del dispositivo è consentita anche la captazione dell'audio della ripresa.

I dati raccolti sono crittografati su memoria non accessibile contenuta nella bodycam.

[OMISSIS]

Gli operatori che hanno effettuato riprese con tali dispositivi dovranno mettere a disposizione del Comando, nel più breve tempo possibile ovvero entro la fine dell'orario di lavoro, apposita relazione di servizio nella quale sarà indicata la sussistenza di riprese relative ai fatti. Il personale autorizzato potrà operare sui filmati esclusivamente mediante il software di gestione, avendo cura di non creare ulteriori copie dei filmati, salvo che ciò non sia richiesto dall'Autorità giudiziaria.

Analoga relazione dovrà essere redatta nel caso di riprese effettuate per errore o per motivi non rientranti nelle finalità del trattamento. In tale ipotesi, l'Ufficiale autorizzato provvederà all'immediata rimozione di tali filmati, attraverso le funzionalità del software di gestione. Lo stesso darà atto con apposita relazione di servizio dell'attività svolta.

Solo il personale autorizzato dal designato al trattamento dei dati ha il permesso di visionare il materiale. Dopo aver accertato che le immagini raccolte riguardino eventi penalmente rilevanti, questo personale procede all'estrazione delle immagini da mettere a disposizione dell'Autorità giudiziaria. Tale attività è opportunamente tracciata e documentata dal software gestionale.

Le immagini sono accessibili esclusivamente dal personale di Polizia locale del Nucleo Informatico e Tecnologico (per le operazioni di consultazione ed esportazione) e dal personale di Polizia locale del Nucleo di Polizia Giudiziaria titolare del fascicolo investigativo.

L'accesso al software gestionale avviene tramite utilizzo di credenziali personali *[OMISSIS]*.

[OMISSIS]

[OMISSIS]

Ogni operazione di accesso, consegna o estrazione dei dati da parte di soggetti autorizzati, verrà opportunamente tracciata e documentata.

6. Estrazione di copie dei dati personali e relative misure di sicurezza.

In nessun caso possono essere eseguite copie dei filmati, se non richieste dall'Autorità giudiziaria.

I dati esportati dalla piattaforma XX sono messi a disposizione dell'avente diritto in due modalità: 1. supporto USB: viene fornita chiavetta USB crittografata [OMISSIS]; 2. supporto CD-DVD: i file sono compressi e crittografati [OMISSIS]. La chiave di decifratura dei dati è fornita all'avente diritto [OMISSIS].

7. Durata della conservazione delle immagini.

Il software di gestione provvederà all'automatica cancellazione irreversibile dei filmati, decorsi sette giorni, salva la presenza di immagini relative a fatti effettivamente pertinenti e rilevanti rispetto alle finalità perseguite. In tal caso, l'operatore incaricato, senza ritardo, attraverso il software gestionale metterà i filmati a disposizione dell'Ufficiale responsabile del Nucleo di Polizia giudiziaria, il quale valuterà la necessità di eventuale conservazione per un tempo superiore ai sette giorni e comunque non superiore a sei mesi, salvo diversa disposizione dell'Autorità giudiziaria procedente.

8. Funzionalità di I.A. impiegate dal sistema.

In sistema XX rende disponibili due funzionalità di AI: Redaction ed Automated People Detection (ADP).

Redaction viene utilizzata per identificare e oscurare automaticamente le informazioni sensibili all'interno delle registrazioni video e audio. Sfruttando algoritmi avanzati di apprendimento automatico, gli strumenti di redazione XX sono in grado di analizzare le riprese per individuare gli attributi o gli elementi che devono essere nascosti. Questo processo semplifica il flusso di lavoro di redazione per le Forze dell'ordine e preserva la privacy delle persone, consentendo alle Forze dell'ordine di condividere le informazioni necessarie senza compromettere i dati sensibili.

La funzione Automated People Detection (ADP), ossia il rilevamento automatico delle persone, è uno strumento che fornisce una vista in miniatura delle persone distinte presenti in un file video. Ciò aiuta gli investigatori a trovare rapidamente i momenti chiave nelle prove digitali, ad esempio saltando al minuto 30 del video quando una persona appare per la prima volta, invece di guardare prima 30 minuti di filmati senza eventi rilevanti. Il rilevamento delle persone non rileva alcuna caratteristica facciale, né assegna identità individuali alle forme umane rilevate. In altre parole, il rilevamento automatico delle persone può dire agli investigatori che, in base alla forma di un oggetto nelle prove digitali, ritiene che quell'oggetto sia generalmente una persona. Tuttavia, non identifica effettivamente quell'individuo, ma si limita a segnalare che nelle prove è visibile un essere umano e, se del caso, che sono presenti più individui distinti.

9. Misure di sicurezza

Tutte le registrazioni a bordo della body cam sono protette mediante stoccaggio su XX allo stato solido, non rimovibile e integrato nella scheda madre, utilizzando un processo di crittografia completa del disco *[OMISSIS]*, le cui chiavi di crittografia sono conosciute esclusivamente dal produttore.

Le videoregistrazioni sono salvate su "cloud dedicato", ospitato nei data center XX situati nell'Unione Europea (Paesi Bassi e Irlanda), fornito e gestito dalla Società XX, nominata formalmente responsabile esterno del trattamento dati; le videoriprese sono visionabili ed estrapolabili esclusivamente dalla piattaforma informatica XX. I dati sulla piattaforma cloud sono protetti da crittografia XX, le cui chiavi crittografiche sono conosciute esclusivamente dal produttore.

La DPIA specifica che "È escluso categoricamente il trasferimento dei dati trattati in territori esterni all'Unione Europea." (pag. 2).

10. Valutazione dei rischi

La DPIA contiene una corretta valutazione dei rischi connessi al trattamento dei dati personali, con individuazione dei singoli rischi, della relativa gravità e probabilità, delle misure adottate per la mitigazione dei rischi, all'esito delle quali si valuta la sussistenza di un rischio residuo di valore medio (pagg. 8-19).

CONSIDERATO

11. Il trattamento di dati personali oggetto della DPIA è finalizzato allo svolgimento, da parte delle autorità competenti, di attività di law enforcement e pertanto è disciplinato dal Decreto.

Come premesso, la DPIA costituisce una nuova versione della precedente, nella quale erano presenti diverse criticità rilevate dall'Ufficio del Garante per quanto riguarda la protezione dei dati personali.

Pur rappresentando un significativo miglioramento rispetto alla precedente, la nuova versione presenta ancora rilevanti problematiche non risolte in modo chiaro, secondo quanto di seguito riportato.

12. Il responsabile del trattamento.

La soluzione di videocamere indossabili in oggetto prevede l'uso del sistema software in cloud XX per la conservazione e l'elaborazione delle riprese.

Il responsabile del trattamento designato dal Comune è la società XX, fornitore e gestore del "cloud dedicato" che eroga il servizio XX (v. pag. 9 della valutazione di impatto).

12.1. Nella DPIA è indicato che l'adozione del servizio XX in cloud comporta che sia le chiavi crittografiche utilizzate per garantire la riservatezza delle registrazioni nelle memorie delle bodycam, che quelle utilizzate per conservare "i dati sulla piattaforma cloud", "sono conosciute esclusivamente dal produttore" (v. pagg. 8 e 9 della valutazione di impatto); ciò comporta una importante cessione di sovranità digitale al soggetto che fornisce ed eroga il servizio. D'altra parte, sebbene sia credibile che il servizio XX in cloud adoperi tecniche crittografiche sia sui dati a riposo che durante la trasmissione (v. anche XX), non sono disponibili sufficienti dettagli tecnici sul processo di gestione delle chiavi crittografiche che consentano di escludere che il fornitore del servizio possa accedere ai dati del titolare in chiaro, in violazione degli articoli 5, comma 1 (in base al quale il trattamento è lecito se è necessario per l'esecuzione di un compito di un'autorità competente per le finalità di cui all'articolo 1, comma 2, del Decreto e si basa sul diritto dell'Unione europea o su disposizioni di legge o di regolamento o su atti amministrativi generali che individuano i dati personali e le finalità del trattamento) e 25 (sicurezza del trattamento) del Decreto.

Inoltre, l'Accordo per la nomina del responsabile del trattamento, allegato alla DPIA, contiene formulazioni ambigue in ordine al trattamento da parte di XX dei dati personali acquisiti dalla Polizia locale di Brescia nell'ambito dello svolgimento di attività di law enforcement. In particolare, nell'allegato 2 all'Accordo, che specifica i dettagli dei trattamenti effettuati per conto del titolare del trattamento (clausola 5 dell'Accordo), è previsto, senza alcuna specificazione, che "i dati raccolti saranno solo trattati da personale autorizzato", senza specificare il tipo di trattamento consentito ai soggetti incaricati e se l'oggetto del trattamento sia costituito da dati personali in chiaro.

12.2. Nel documento XX (Informativa sulla privacy dei servizi cloud XX), al quale si accede attraverso il link del servizio XX, indicato a pagina 9 della DPIA (XX), è indicato che tale informativa riguarda anche i servizi cloud erogati da XX tra cui, appunto, XX. In relazione a tali servizi, l'informativa dichiara che "XX and its other legal entities" sono i data processor dei contenuti caricati dai clienti nel cloud dei suoi servizi, e data controller per i "Non-Content Data". I "Non-Content Data" consistono nei dati relativi all'organizzazione cliente e ai suoi utenti (assimilabili, si ritiene, al personale abilitato al trattamento), i "Customer Entity and User Service Interaction Data", gli "Account Data", i "Support Data".

In relazione alle diverse tipologie di dati a vario titolo trattate, XX dichiara che i contenuti dei clienti restano confinati nella specifica "economic area", mentre i "Non-Content data" possono essere

ubicati o trasferiti al di fuori dello Spazio economico europeo (SEE) (“Personal Data within Non-Content Data may be subject to international data transfers outside the European Economic Area (EEA)”).

L’informativa prevede altresì che “XX può condividere i dati con le sue controllate, entità legali, fornitori di servizi di terze parti e altri partner per aiutarci a operare, anche per i fornitori per facilitare: (1) gestione dell'account utente, autenticazione, analisi e comunicazione, (2) caratteristiche del prodotto, ad esempio sviluppo del prodotto e analisi degli errori, (3) servizio clienti e supporto e (4) monitoraggio e indagine della sicurezza.” (“XX may share data with its subsidiaries, legal entities, third party service providers and other partners to help us operate, including for providers to facilitate: (1) user account management, authentication, analytics, and communication, (2) product features, e.g. product development, and error analytics, (3) customer service and support, and (4) security monitoring and investigation.”).

12.3 In ordine ai content data, l’Accordo per la nomina di XX a responsabile “esterno” del trattamento dei dati (di seguito anche “Accordo”), prodotto a corredo della DPIA (all. 06), indica, a proposito dei trasferimenti internazionali, che “il responsabile del trattamento e il sub-responsabile del trattamento possono devono garantire il rispetto del capo IV Decreto Legislativo n.51/2018. In particolare il responsabile deve darne notizia al titolare per gli adempimenti previsti dall’art. 33 del Decreto Legislativo n.51/2018”. Tuttavia, in esso si precisa che “Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo IV del D. Lgs. 51/2018.”. Ciò è comprensibile, in quanto le clausole contrattuali conferiscono solo diritti contrattuali agli interessati nei confronti delle entità che hanno firmate; peraltro, il meccanismo delle clausole contrattuali-tipo non è contemplato dalla Direttiva 680/2016 e dal Decreto, onde è inconferente nell’ambito del trattamento dei dati de quo.

L’XX cloud services privacy notice, già citato, specifica che XX non divulgherà il contenuto del cliente o i dati non relativi al contenuto alle Autorità governative, ad eccezione di quanto richiesto da qualsiasi legge o regolamento. Se consentito, XX notificherà al Cliente se viene ricevuta una richiesta di divulgazione per il Contenuto del Cliente in modo che il Cliente possa contestare o opporsi (“Required Disclosures - XX will not disclose Customer Content or Non-Content Data to Government Authorities except as required by any law or regulation. If permitted, XX will notify Customer if any disclosure request is received for Customer Content so Customer may challenge or object.”).

Le FAQ pubblicate da XX (XX) confermano che se un ente governativo, nazionale o estero, richiede i dati dei clienti presenti su XX, deve seguire la procedura legale applicabile, notificando ad XX un'ordinanza del tribunale per i contenuti o una citazione in giudizio per informazioni. XX reindirizzerà tali richieste al cliente proprietario dei dati. Se obbligata a divulgare i dati, XX ne darà comunicazione al cliente e fornirà una copia della richiesta, a meno che non vi sia un divieto legale (“If a government, domestic or foreign, demands Customer Data residing within XX, it must follow the applicable legal process, serving XX with a court order for content or a subpoena for information. XX would redirect such requests to the customer that owns the data. If compelled to disclose data, XX would notify the customer and provide a copy of the demand, unless legally prohibited from doing so.”).

In tale contesto, rileva: la circostanza che XX conosca le chiavi crittografiche utilizzate per garantire la riservatezza delle registrazioni nelle memorie delle bodycam e conservare i dati sulla piattaforma cloud, onde non si può escludere che il fornitore del servizio possa accedere ai dati del titolare in chiaro; la mancanza di chiarezza in ordine ai rapporti esistenti tra la Società *[OMISSIS]*, rapporti della cui esistenza si ha evidenza per la presenza, nella pagina web messa a disposizione da XX per l’accesso al servizio dal parte del Comune di Brescia, di un link che rinvia alla XX cloud services privacy notice della società americana; la natura globale delle infrastrutture dei fornitori di servizi in cloud, non consentono di escludere che i dati in argomento possano

essere richiesti ed ottenuti sulla base di ordini o richieste di autorità pubbliche di Paesi terzi in assenza delle condizioni stabilite dal capo IV del Decreto. Dall'esame delle DPIA e dei documenti allegati non risulta che il Comune di Brescia abbia adeguatamente preso in considerazione tale criticità.

12.4. Circa i non-content data, l'Accordo è estremamente generico; in esso è indicato (allegato II) che "nella misura in cui i dati di utilizzo (compresi i log e i metadati delle query) e/o i dati operativi (compresi i dati di fatturazione e di assistenza) in relazione all'uso dei Servizi da parte del Cliente (collettivamente "Dati di Utilizzo e Operativi") siano considerati Dati Personali, XX è un Titolare autonomo dei dati e Tratterà tali dati in conformità al Contratto e alla Normativa Privacy applicabile per sviluppare, migliorare, supportare e gestire i propri prodotti e servizi. A fini di chiarezza, XX non divulgherà a terzi alcun Dato di Utilizzo e Operativo che includa Informazioni Confidenziali del Cliente se non (a) in conformità alle relative disposizioni di riservatezza contenute nel Contratto, o (b) nella misura in cui i Dati di Utilizzo e Operativi siano, in conformità alla Normativa Privacy, anonimizzati, de-identificati e/o aggregati in modo tale da non poter più identificare direttamente o indirettamente il Cliente o alcun particolare soggetto.

Tali definizioni in ordine alla natura dei "Dati di Utilizzo e "dati Operativi" sono generiche e meramente esemplificative ("compresi i …"), al punto in cui la stessa qualificazione dei medesimi in termini di dato personale è dubitativa ("nella misura in cui […] siano considerati Dati Personali"). Senza una indicazione di dettaglio in ordine ai tipi di dati personali trasferiti ad XX, il titolare del trattamento non può valutare la sussistenza di misure necessarie per garantire la continuità della loro protezione una volta trasferiti. Anche le finalità di tale trasferimento indicate da XX sono del tutto generiche ("sviluppare, migliorare, supportare e gestire i propri prodotti e servizi"). Né è indicato, tra l'altro, se le predette finalità siano nell'interesse del Comune titolare, oppure nell'esclusivo interesse di XX, ossia se attengano ai servizi commerciali prodotti e/o forniti da XX ancorché non compresi nella fornitura al Comune del servizio XX.

La predetta mancanza di granularità delle informazioni presenti nell'accordo non consente al titolare del trattamento (Comune di Brescia) di valutare il rispetto dell'articolo 5 del Decreto, secondo cui il trattamento dei dati personali da parte del titolare, compresa la cessione, è lecito se è necessario per l'esecuzione di un compito di un'autorità competente per le finalità law enforcement, e si basa sul diritto dell'Unione europea o su disposizioni di legge o di regolamento o su atti amministrativi generali che individuano i dati personali e le finalità del trattamento, nonché dell'articolo 6, comma 1, del Decreto, secondo cui i dati personali raccolti per le finalità di law enforcement non possono essere trattati per finalità diverse, salvo che tale trattamento sia consentito dal diritto dell'Unione europea o dalla legge.

Quanto ad eventuali trasferimenti dei non content data in Paesi terzi, né l'Accordo, né l'ulteriore documentazione fornita dal titolare lo escludono; al contrario, questi sono espressamente previsti nell'XX Cloud Services Privacy Notice, come sopra rilevato.

13. Il sub-responsabile.

L'Accordo per la nomina di XX a responsabile del trattamento sancisce il divieto di "sub contrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento".

13.1. Orbene, l'allegato IV dell'Accordo si limita e si sostanzia in una tabella denominata "elenco dei sub responsabili del trattamento", che indica XX quale "sub-responsabile di infrastrutture di terze parti" e indica quale "Ubicazione del Data Center: Paesi Bassi, Irlanda.".

Non è stata fornita alcuna informazione sulle operazioni di trattamento che XX intende affidare al

predetto sub-responsabile.

Inoltre, nonostante l'Accordo preveda che XX debba fornire al titolare del trattamento le informazioni necessarie per consentirgli di decidere in merito all'autorizzazione della nomina del sub responsabile (par. 7.7.), non risulta che tali informazioni siano state fornite o, se fornite, valutate dal Comune.

Pertanto il Comune, al quale compete, in qualità di titolare del trattamento, la decisione finale in merito al ricorso a uno specifico sub-responsabile del trattamento e la relativa responsabilità, non ha dimostrato di avere effettuato una verifica dell'adeguatezza delle garanzie fornite dai sub-responsabili del trattamento, verifica che deve essere particolarmente approfondita per i trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, come quelli in argomento (Cfr. Parere dell'EDPB 22/2024 su taluni obblighi derivanti dal ricorso a uno o più responsabili del trattamento e a uno o più sub-responsabili del trattamento, adottato il 7 ottobre 2024 https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202422_relianceonprocessors-sub-processors_it_0.pdf.).

13.2. Il medesimo allegato IV relativo alla designazione del sub-responsabile contiene un "Link Esterno con Informazioni Aggiuntive" (XX), che conduce alla "Informativa sulla privacy di XX", il cui sottoparagrafo intitolato "Dove sono memorizzati ed elaborati i dati personali", stabilisce che (XX): "I dati personali raccolti da XX possono essere archiviati ed elaborati nella regione dell'utente, negli Stati Uniti e in qualsiasi altra giurisdizione in cui XX o le sue affiliate, filiali o fornitori di servizi gestiscono strutture. XX gestisce i principali data center in Australia, Austria, Brasile, Canada, Finlandia, Francia, Germania, Hong Kong, India, Irlanda, Giappone, Corea, Lussemburgo, Malaysia, Paesi Bassi, Singapore, Sudafrica, Regno Unito e Stati Uniti. In genere, la posizione di archiviazione principale è nell'area geografica del cliente o negli Stati Uniti, spesso con un backup in un data center in un'altra area geografica. Le posizioni di archiviazione sono scelte per operare e fornire i servizi in modo efficiente, migliorare le prestazioni e creare ridondanze per proteggere i dati in caso di interruzioni o altri problemi. Vengono adottate le misure necessarie per elaborare i dati raccolti in base alla presente informativa sulla privacy, in base alle disposizioni della presente informativa e ai requisiti della legge applicabile. I dati personali vengono trasferiti dal paese di raccolta originario ad altri paesi, alcuni dei quali non sono ancora stati determinati dalla Commissione europea o da un'altra autorità di protezione dei dati applicabile nella propria area geografica per un livello adeguato di protezione dei dati. Ad esempio, le leggi potrebbero non garantire gli stessi diritti oppure potrebbe non esserci un'autorità di vigilanza sulla privacy in grado di risolvere meccanismi e misure di sicurezza legali, tra cui contratti come le clausole contrattuali standard pubblicate dalla Commissione Europea ai sensi della decisione di implementazione della Commissione 2021/914, per contribuire alla protezione dei diritti dell'utente e consentire a tali protezioni di spostarsi con i dati dell'utente.".

Ancorché l'Accordo preveda, come già rilevato, che, a proposito dei trasferimenti internazionali, "responsabile del trattamento e il sub-responsabile del trattamento possono devono garantire il rispetto del capo IV Decreto Legislativo n.51/2018. In particolare il responsabile deve darne notizia al titolare per gli adempimenti previsti dall'art. 33 del Decreto Legislativo n.51/2018", nel medesimo atto si precisa che "Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo IV del D. Lgs. 51/2018.". Ciò è comprensibile, in quanto le clausole contrattuali conferiscono solo diritti contrattuali agli interessati nei confronti delle entità che hanno firmate. Tuttavia, ciò che rileva maggiormente è che il meccanismo delle clausole contrattuali tipo non è contemplato dalla Direttiva 680/2016 e dal Decreto, onde è inconferente nell'ambito del trattamento dei dati de quo.

Come ha osservato l'European Data Protection Supervisor, l'applicazione extraterritoriale delle leggi di Paesi terzi che concedono l'accesso ai dati trattati dai fornitori di servizi cloud comporta un rischio per l'effettiva conformità alle disposizioni europee in materia di privacy. Tale rischio

sussiste non solo per i dati personali trasferiti o in corso di trasferimento verso Paesi terzi, ma anche per quelli trattati esclusivamente nello SEE. Data la natura globale dell'infrastruttura e delle risorse dei fornitori di servizi cloud multinazionali o iper-scala, l'accesso da altre giurisdizioni è una probabilità prevedibile (cfr. EDPS investigation into use XX by the European Commission, Case 2021-0518, par. 529).

Oltre a quanto sopra riportato, si ricorda che nell'ambito di applicazione del Decreto, il trasferimento di dati personali in Paesi terzi è possibile – sempre che sussistano le condizioni ivi previste – solo ove avvenga nei confronti di un titolare del trattamento o un'organizzazione internazionale che sia un'autorità competente per le finalità di law enforcement di cui all'articolo 1 dello stesso Decreto (cfr. art. 31 del Decreto). Ancorché, l'articolo 35 del Decreto consenta trasferimenti di dati personali da parte di un'autorità competente di uno Stato membro UE verso singoli destinatari in Paesi terzi diversi dalle autorità competenti, tale facoltà è sottoposta a vincoli specifici fra i quali, in primis, la stretta necessità del trasferimento per assolvere un compito previsto dal diritto UE o nazionale e, soprattutto, la natura non sistematica bensì occasionale e specifica del trasferimento, circostanza quest'ultima che evidentemente non è soddisfatta nel caso specifico della scelta di un sub-responsabile operante su base permanente per conto di XX.

14. Le criticità sopra rilevate sono già state evidenziate – in linea generale - nel Rapporto sull'azione coordinata di applicazione (CEF) 2022 del Comitato europeo per la protezione dei dati (https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud basedservices_publicsector_en.pdf), avente ad oggetto "l'uso del cloud nel settore pubblico", con particolare riferimento alla valutazione del rischio, al ruolo delle parti, alla disponibilità delle chiavi di cifratura, alla difficoltà di negoziare un contratto personalizzato, alla conoscenza o al controllo da parte degli enti pubblici titolari sui sub-responsabili del trattamento, e ai trasferimenti internazionali e all'accesso da parte di autorità pubbliche straniere.

15. Dall'esame della DPIA e dei documenti allegati si è indotti a ritenere che la scelta del servizio in cloud per la custodia e gestione dei dati personali abbia preceduto - e non fatto seguito - le valutazioni in ordine alle misure necessarie per assicurare il pieno rispetto della normativa in materia di protezione dati, specie sotto il profilo della sicurezza dei dati personali oggetto di trattamento. In effetti, dall'Accordo di designazione del responsabile del trattamento risulta che il Comune di Brescia aveva acquisito "n. 35 XX con n. 1 licenza d'uso annua del software XX e n. 34 licenze d'uso annue del software basic con soluzione cloud per apposizione certificati sui filmati" già nel giugno 2022, ossia prima della richiesta di consultazione preventiva sottoposta a questa Autorità. Del resto, il Comune non ha chiarito se la scelta dello specifico prodotto fornito da XX sia scaturita da una valutazione comparativa con altre soluzioni presenti nel mercato ed in che modo tale scelta abbia tenuto conto degli aspetti di protezione dei dati personali connessi alla natura ad elevato rischio del trattamento in argomento.

16. Conclusioni.

Per quanto sopra rilevato, la DPIA del Comune di Brescia ed i documenti che la integrano, valutati anche sulla base della ulteriore documentazione acquisita in fase istruttoria, non appaiono conformi alla disciplina in materia dei dati personali, per i seguenti motivi:

a) per avere consentito, il Comune di Brescia, che le chiavi crittografiche utilizzate, sia per garantire la riservatezza delle registrazioni nelle memorie delle bodycam, che quelle utilizzate per conservare i dati sulla piattaforma cloud, siano conosciute esclusivamente dal produttore senza potere escludere che il fornitore del servizio possa accedere ai dati del titolare in chiaro, in violazione degli articoli 5, comma 1 e 25 del Decreto (punto 12.1);

b) per non avere, il Comune di Brescia, verificato l'assenza del rischio del trasferimento dei content data in Paesi terzi in violazione del capo IV del Decreto (punto 12.3);

c) per non avere, il Comune di Brescia, richiesto al responsabile del trattamento informazioni adeguate in ordine ai non-content data per i quali quest'ultimo è riconosciuto titolare del trattamento, con conseguente mancata valutazione del rispetto dell'articolo 5 del Decreto, secondo cui il trattamento dei dati personali, compresa la cessione, è lecito se è necessario per l'esecuzione di un compito di un'autorità competente per le finalità di law enforcement, e si basa sul diritto dell'Unione europea o su disposizioni di legge o di regolamento o su atti amministrativi generali che individuano i dati personali e le finalità del trattamento, nonché dell'articolo 6, comma 1, del Decreto, secondo cui i dati personali raccolti per le finalità di law enforcement non possono essere trattati per finalità diverse, salvo che tale trattamento sia consentito dal diritto dell'Unione europea o dalla legge (punto 12.4);

d) per la mancata verifica, da parte del Comune di Brescia, che il trasferimento in Paesi terzi dei non-content data avvenga nel rispetto delle condizioni di cui al capo IV del Decreto (punto 12.4);

e) per la mancata valutazione, da parte del Comune di Brescia, delle informazioni necessarie per autorizzare il responsabile del trattamento a ricorrere ad un sub-responsabile del trattamento e per la mancata verifica dell'adeguatezza delle garanzie fornite dai sub-responsabili (art. 18, comma 1, del Decreto) (punto 13.1).

f) per la mancata verifica, da parte del comune di Brescia, che il sub-responsabile del trattamento non comunichi dati personali a soggetti stabiliti in Paesi terzi senza che ricorrano le condizioni di cui al Capo IV del Decreto (punto 13.2).

Deve, infine, rilevarsi che non sono stati chiariti rapporti, sinergie e collegamenti esistenti tra la Società XX e la Società statunitense XX, rapporti della cui esistenza si ha evidenza per la presenza, nella pagina web messa a disposizione da XX per l'accesso al servizio da parte del Comune di Brescia, di un link che rinvia alla XX cloud services privacy notice della società americana, come sopra già indicato.

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 Brescia, relativa ad un sistema videocamere operative individuali (body cam) da fornire in dotazione agli agenti della Polizia locale, per le ragioni esplicitate in motivazione e richiamate nel punto 16.

Roma, 11 giugno 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Montuori