Regolamento generale europeo sulla protezione dei dati (GDPR)

Implicazioni per la videosorveglianza

Indice

Il Regolamento generale europeo sulla protezione dei dati (GDPR, General Data Protection Regulation) entra in vigore il 25 maggio 2018. Il suo scopo è dare alle persone un maggiore controllo sulla raccolta, sul trattamento e sulla condivisione dei loro dati. Questo ha implicazioni per gli installatori, gli integratori di sistemi e gli utenti delle tecnologie di videosorveglianza.

Il GDPR ha una struttura che aiuta a chiarire ruoli e responsabilità nelle imprese e dà alle persone più possibilità di controllare l'uso dei loro dati.

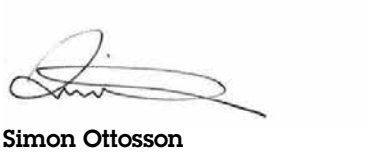
Il regolamento disciplina sia le organizzazioni che hanno sede nell'Unione europea (UE) sia quelle che trattano e conservano i dati personali di soggetti che risiedono nell'Unione, indipendentemente da dove si trovi l'organizzazione.

Come impresa, Axis si è sempre impegnata a rispettare e salvaguardare la privacy personale. Di conseguenza, Axis è pienamente favorevole all'introduzione del GDPR e, mentre si impegnerà a osservarlo rigorosamente, offrirà assistenza ai clienti per agevolarne la conformità nel miglior modo possibile.

Axis ha preso una serie di provvedimenti per adottare un modello di conformità al GDPR. Parte di questa strategia prevede verifiche e revisioni costanti per garantire che le attività svolte da Axis in materia di trattamento dei dati rimangano sicure.

Molte organizzazioni hanno domande sul GDPR. Perché occorre un nuovo regolamento? Che cosa comporta? Che effetti ha sulla videosorveglianza? Quali procedure seguire per essere conformi?

Questo documento tecnico esamina tutte le implicazioni del GDPR e intende aiutare tutti gli operatori nel settore della videosorveglianza a fronteggiare criticità e opportunità.



Simon Ottosson
Legal counsel
Axis Communications

Edwige Maury
Regional Director - Southern Europe
Axis Communications

1. Che cos'è il GDPR?

Il Regolamento generale sulla protezione dei dati (GDPR) è un complesso di regole che disciplina tutti i tipi di dati personali conservati da un'organizzazione. Il GDPR garantisce a ogni individuo la proprietà dei suoi dati personali. Per quanto riguarda l'organizzazione che li detiene, introduce una responsabilizzazione in tutte le fasi del trattamento e della conservazione dei dati. A questo scopo, il GDPR concede vari diritti alle persone e impone obblighi corrispondenti alle organizzazioni che trattano i loro dati.

Cosa sono i dati personali?
Per capire il GDPR occorre una chiara definizione legale di "dati personali". La legge definisce "dati personali" tutte le informazioni relative a una persona identificata o identificabile. Una persona identificabile è un soggetto che può essere identificato direttamente o indirettamente, in particolare facendo riferimento a elementi come nome, numero identificativo, dati geografici, identificatori online come indirizzi IP o cookie, oppure a uno o più fattori specifici di identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale.

Ambito geografico del GDPR
Il GDPR si applica sempre al trattamento dei dati personali da parte di un'azienda che ha sede nell'Unione europea. Qualora l'azienda non abbia sede nell'Unione europea, il GDPR si applica se i dati trattati riguardano persone che si trovano nell'Unione, se il trattamento dei dati è relativo all'offerta di beni e servizi a tali persone quando si trovano nell'Unione o se è riferito al monitoraggio del comportamento delle persone quando si trovano nell'Unione europea. Dunque, il regolamento europeo ha un'evidente portata globale.

Le varie responsabilità per le organizzazioni
Tutte le organizzazioni che trattano o conservano dati personali devono assumersi la responsabilità di garantire la conformità delle loro operazioni al GDPR.

Il GDPR classifica le organizzazioni in due categorie: *titolari del trattamento dei dati* e *responsabili del trattamento dei dati*. Ognuna ha i propri obblighi legali:

Titolari del trattamento: il titolare del trattamento è chi determina lo scopo e le modalità di trattamento dei dati personali. Ad esempio, può essere il proprietario di un punto vendita che utilizza un sistema TVCC per finalità di sorveglianza.

Responsabili del trattamento: il responsabile del trattamento è chi tratta i dati personali per conto del titolare del trattamento e secondo le sue istruzioni. Un responsabile del trattamento può essere un'azienda che gestisce i dati raccolti da un sistema TVCC per conto e secondo le istruzioni di una persona che possiede il sistema di sorveglianza, ad esempio il titolare di un punto vendita.

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
Secondo il GDPR, il titolare del trattamento ha l'obbligo di adottare misure tecniche od organizzative specifiche per implementare i principi di tutela dei dati definiti dal documento. Il GDPR definisce questo concetto *protezione dei dati fin dalla progettazione*. Nel caso di una telecamera (firmware compreso), un esempio rilevante di protezione dei dati fin dalla progettazione potrebbe essere una funzione che consenta digitalmente all'utente di limitare l'acquisizione delle immagini a un certo perimetro, impedendo alla telecamera di acquisire immagini esterne ad esso.

Il titolare del trattamento ha anche l'obbligo di adottare misure tecniche od organizzative che, per default, garantiscano il trattamento meno intrusivo possibile dei dati personali ai fini della privacy: il GDPR definisce questo concetto *protezione per impostazione predefinita*. Nel caso di una telecamera (firmware compreso), un esempio rilevante di protezione per impostazione predefinita potrebbe essere una funzionalità che inviti automaticamente un utente a impostare il perimetro esatto di acquisizione dell'immagine, come nell'esempio riportato sopra.

Il diritto delle persone
Una delle principali forze trainanti del GDPR è l'esigenza di garantire alle persone una maggiore protezione e una serie di diritti che regolamentino i loro dati. Ai sensi del regolamento, requisiti molto specifici impongono alla parte che tratta o archivia i dati personali il dovere di mantenerli riservati.

Il regolamento concede anche alle persone il diritto di essere informate della raccolta dei dati in ogni punto di acquisizione e delle modalità di utilizzo dei dati. Nel caso della videosorveglianza, ad esempio, questo significa esporre opportuni cartelli nell'area monitorata e in quelle circostanti.

2. Come incide sulla videosorveglianza il GDPR?

Molti dibattiti sul GDPR si sono incentrati sulla conservazione e sul trattamento in sicurezza di dati più tradizionali, come gli elenchi di nomi e indirizzi e-mail in fogli di calcolo o database. Si è parlato molto meno dei filmati, ma le aziende devono esserne altrettanto consapevoli.

Nella misura in cui contenga dati personali, la videosorveglianza è soggetta alle disposizioni del GDPR.

Effetti del GDPR sull'uso delle apparecchiature di sorveglianza (telecamere e soluzioni)
Per quanto riguarda i prodotti e le soluzioni commercializzate da Axis, è l'utente (in quanto titolare del trattamento) ad avere la responsabilità di garantire che qualsiasi utilizzo che preveda il trattamento dei dati personali sia conforme al GDPR. Questo significa che, nel caso dei prodotti e delle soluzioni, la conformità o eventuali infrazioni del GDPR dipendono in genere dall'uso che ne fa il cliente.

Effetti del GDPR sull'uso di servizi hosted specifici
Nel caso dei servizi, la conformità al GDPR dipende in una certa misura dalle modalità di prestazione del servizio: questa responsabilità è di Axis. Tuttavia, la conformità o eventuali infrazioni del GDPR dipendono in gran parte dalle modalità di utilizzo del servizio da parte dei clienti. Gli obblighi derivanti dal GDPR e le persone ad essi vincolate devono essere esaminati specificamente per ogni applicazione.

Prendiamo ad esempio un servizio hosted, AXIS Guardian. Di seguito sono elencate le modalità di applicazione del GDPR, le responsabilità e i responsabili:

> *Clienti dell'operatore del sistema di allarme:* titolari del trattamento dei dati personali contenuti nel materiale video acquisito dal sistema di sorveglianza dell'utente e caricato in AXIS Guardian.
> *Operatore del sistema di allarme:* responsabile del trattamento, per conto degli utenti, dei dati personali caricati in AXIS Guardian dall'utente (es. informazioni sui dipendenti dell'utente e video acquisito).
> *Axis:* responsabile del trattamento, per conto dell'operatore del sistema di allarme, dei dati personali caricati in AXIS Guardian dall'operatore (es. informazioni sui dipendenti dell'operatore). Inoltre, sub-responsabile dei dati personali, per conto dell'operatore del sistema di allarme, dei dati personali caricati in AXIS Guardian dai clienti dell'operatore (filmati acquisiti).
> *Amazon Web Services:* sub-responsabile del trattamento, per conto di Axis, dei dati personali caricati in AXIS Guardian dall'operatore del sistema di allarme e dai clienti dell'operatore (utenti).

2.1 Procedure per la conformità al GDPR

Il GDPR è un regolamento che influenzerà il trattamento dei dati (anche video) da parte delle organizzazioni.

Come requisito minimo, ogni organizzazione che tratta dati personali dovrà designare uno o più responsabili per verificare che siano gestiti in conformità al GDPR e alla politica dell'azienda (il numero di incaricati dipende dalle dimensioni dell'impresa e dalla quantità di dati personali raccolti e trattati). Inoltre, per alcune organizzazioni il GDPR richiede la nomina formale di un responsabile della protezione dei dati (DPO, Data Protection Officer) per tali attività.

Sono inoltre previsti cambiamenti nel processo amministrativo. Ai sensi del GDPR, le organizzazioni devono tenere registri dettagliati e accurati delle attività di trattamento dei dati. È obbligatorio registrare una serie di dati tra cui (a titolo esemplificativo):

> La categoria di persone alla quale si riferiscono i dati personali trattati (es. clienti, dipendenti, visitatori in negozio, ecc.)
> Le finalità per le quali si utilizzano i dati personali
> L'eventuale trasferimento dei dati personali ad altre aziende e/o fuori dall'Unione europea
> Il periodo di conservazione dei dati personali
> Le misure adottate dall'organizzazione per ogni singola attività di trattamento dei dati per garantire la conformità al GDPR

Quanto elencato sopra è rilevante per la videosorveglianza archiviata.

Le organizzazioni sono obbligate a spiegare perché una telecamera si trovi in un particolare punto, che cosa viene ripreso e perché. Nel caso della videosorveglianza, è necessario esporre opportuni cartelli nell'area monitorata e in quelle circostanti.

Il titolare del trattamento può essere obbligato a condurre una valutazione d'impatto sulla protezione dei dati (DPIA, Data Protection Impact Assessment) prima di installare una telecamera in un luogo pubblico. La valutazione deve includere (voci da stabilire specificamente a seconda dei casi):

> Descrizione sistematica delle operazioni di trattamento previste e delle finalità del trattamento
> Valutazione della necessità e della proporzionalità delle operazioni di trattamento in rapporto alle finalità
> Valutazione dei rischi per i diritti e la libertà delle persone
> Misure previste per contrastare tali rischi, compresi meccanismi e garanzie per assicurare la protezione dei dati personali e la conformità al GDPR (tenendo in considerazione i diritti e gli interessi legittimi delle persone e di altre figure coinvolte)

Uno dei punti fermi del nuovo regolamento è che le persone monitorate devono essere pienamente informate sul tipo di dati conservati e sulle modalità di utilizzo.

Il regolamento definisce chiaramente alcune regole basilari sulla crittografia e sulle modalità di protezione dei dati. Il fatto che i dati siano disponibili sotto forma di video non altera questo requisito.

Le aziende che archiviano i video, dunque, hanno responsabilità chiare per quanto riguarda la custodia dei dati personali e devono adottare misure efficaci per prevenire gli accessi non autorizzati. Questo significa che è importante definire per iscritto chi avrà accesso alle telecamere e alle registrazioni.

Le organizzazioni devono anche prevedere un'apposita procedura se una persona sceglie di esercitare il suo diritto ad accedere ai dati personali o ne richiede la cancellazione. In tal modo, possono rispettare la scadenza di un mese entro la quale devono soddisfare queste richieste, come previsto dal GDPR. In questi casi è ragionevole aspettarsi che il richiedente fornisca informazioni accurate per individuare i dati, indicando ad esempio un intervallo temporale preciso e il luogo in cui sono state acquisite le riprese.

Le aziende devono adottare misure efficaci per prevenire gli accessi non autorizzati ai dati personali che custodiscono. Le strategie utilizzate da ogni azienda varieranno in base alle singole criticità; tuttavia, in tutti i casi le aziende dovranno svolgere controlli di sicurezza efficaci, adottare prassi ottimali e aggiornate per la cyber security e lavorare con partner affidabili che forniscano hardware/software sicuri e un'assistenza completa.

3. Conclusioni

In ultima battuta, è l'utente delle apparecchiature, delle soluzioni e dei servizi di sorveglianza a essere responsabile della conformità al GDPR e della salvaguardia dei diritti delle persone di cui tratta i dati. Le organizzazioni che in questo senso hanno fatto poco o niente dovranno adeguarsi al più presto. Quelle che invece hanno agito preventivamente e prestato attenzione alle responsabilità definite dal regolamento hanno meno da preoccuparsi.

Per gli utenti di apparecchiature, soluzioni e servizi di sorveglianza, è dunque importante collaborare con fornitori e rivenditori che si impegnino a rispettare e salvaguardare la privacy e a tutelare i dati personali. Inoltre, occorre anche poter contare sull'aiuto e sull'assistenza tecnica di fornitori e rivenditori per agevolare la conformità al GDPR.

Materiali supplementari:

Dettagli completi sul GDPR

Sito del Garante europeo della protezione dei dati

Sito della Guida alla protezione dei dati per piccole e medie imprese

72047/IT/R1/1807

Informazioni generali su Axis Communications

Axis rende possibile un mondo più intelligente e sicuro creando soluzioni di rete che forniscono informazioni utili per aumentare la sicurezza e trovare nuovi modi di fare business. In qualità di leader nel video di rete, Axis offre prodotti e servizi per la videosorveglianza, il controllo accessi, i sistemi audio e le analisi video.

Axis ha più di 2800 dipendenti dedicati in oltre 50 paesi e collabora con partner di tutto il mondo per offrire le migliori soluzioni ai clienti. Fondata nel 1984, Axis è una società con sede in Svezia e quotata all'indice NASDAQ di Stoccolma con la sigla AXIS.

Per ulteriori informazioni su Axis, visitare il sito web www.axis.com.

AXIS COMMUNICATIONS