Reglamento general de protección de datos de la UE (GDPR)

Implicaciones para el sector de la videovigilancia

AXIS COMMUNICATIONS

Tabla de contenidos

El Reglamento General para Protección de Datos (GDPR) de la UE entra en vigor el 25 de mayo de 2018. Su objetivo es ofrecer a las personas un mayor control sobre la recopilación, el procesamiento y la distribución de los datos de los individuos, algo que tiene implicaciones para instaladores, integradores de sistemas y usuarios de tecnología para videovigilancia.

El GDPR proporciona una estructura que ayuda a clarificar los cargos y las responsabilidades en las empresas y también ofrece a los individuos más oportunidades para controlar el uso de sus datos personales.

El reglamento se dirige a las organizaciones con sede en la Unión Europea (UE) y a aquellas que procesan y guardan los datos personales de las personas que residen en esta misma región, independientemente del emplazamiento de la organización.

Como compañía, Axis se ha comprometido siempre con el respeto y la protección de la privacidad de las personas y, teniendo esto presente, apoya firmemente la puesta en marcha del GDP, colaborando para su cumplimiento dentro de la compañía y proporcionando soporte a sus clientes para facilitar su cumplimiento de la mejor forma posible.

Axis ha dado unos pasos importantes para la implementación de un modelo para el cumplimiento del GDPR. Como parte de esta estrategia, se incluyen las pruebas y las revisiones constantes llevadas a cabo para garantizar la seguridad permanente de las actividades que realiza Axis en relación al procesamiento de los datos.

Muchas organizaciones tienen preguntas relacionadas con el GDPR. ¿Por qué necesitamos ahora este nuevo reglamento? ¿Qué implica? ¿Cómo va a afectar a la videovigilancia? ¿Qué pasos deberían darse para garantizar el cumplimiento?

Este documento explora las implicaciones del GDPR y tiene como objetivo ayudar a las empresas del sector de la videovigilancia para orientarles en los retos y las oportunidades que va a presentar la puesta en marcha del GDPR.

Simon Ottosson
Asesor legal
Axis Communications

Edwige Maury
Regional Director - Southern Europe
Axis Communications

1. ¿Qué es el GDPR?

El Reglamento General para Protección de Datos (GDPR) de la UE es un conjunto de normas que se aplican a todos los tipos de datos personales guardados en cualquier organización. El GDPR proporciona a todos los individuos la propiedad de sus datos personales y, por parte de las organizaciones, introduce un alto grado de responsabilidad en todas las etapas del procesamiento y el almacenamiento de los datos. El GDPR logra estos objetivos ofreciendo una serie de derechos a las personas y estableciendo ciertas obligaciones para las organizaciones encargadas del procesamiento de los datos.

¿Qué se entiende por datos personales?
Una parte esencial para entender el GDPR es dejar clara la definición legal de datos personales. La legislación define los datos personales como cualquier información relacionada con una persona identificada o identificable. Una persona identificable es cualquier individuo que pueda identificarse de forma directa o indirecta, en particular en referencia a un elemento identificador como el nombre, un número de identificación, datos sobre emplazamiento, un identificador online como una dirección IP o un identificador de cookies, o uno o más factores específicos relacionados con la información física, genética, mental, económica, cultural o social de esa persona.

Ámbito geográfico del GDPR
El GDPR siempre se aplica al procesamiento de los datos personales por una compañía siempre que dicha compañía se encuentre en la UE, y el GDPR se aplica si los datos procesados son de personas que se encuentran en la UE, si el procesamiento de los datos guarda relación con el suministro de bienes o servicios a estas personas cuando están en la UE o si la monitorización de dichas personas se realiza cuando se encuentran en la UE. De ahí que, claramente, este reglamento europeo tenga un impacto mundial.

Diferentes responsabilidades para las organizaciones
Cualquier organización que procese o almacene datos personales debe responsabilizarse de realizar estas tareas cumpliendo con el GDPR.

El GDPR clasifica las organizaciones en dos categorías: controladores de datos, y procesadores de datos, cada una de ellas con sus propias obligaciones legales:

Controladores de datos: Un controlador de datos es cualquier persona que determina el fin y los medios para el procesamiento de datos personales, como, por ejemplo, un propietario de un establecimiento que usa un sistema de CCTV para vigilancia.

Procesadores de datos: Un procesador de datos es cualquier persona que procesa datos personales en nombre y de acuerdo con las instrucciones que proporciona el controlador de datos. Un procesador puede ser una compañía que gestiona los datos recopilados por un sistema de CCTV en nombre y de acuerdo con las instrucciones proporcionadas por alguien que tiene un sistema de CCTV para vigilancia, como, por ejemplo, el propietario de un establecimiento.

Privacidad mediante diseño y privacidad por defecto
Según el GDPR, el controlador de datos personales, cuando procese dichos datos, tiene la obligación de implementar medidas técnicas u organizativas diseñadas para poner en marcha los principios para protección de datos establecidos en el GDPR. El GDPR se refiere a esto como privacidad mediante diseño. En el contexto de una cámara que incluye firmware, un ejemplo relevante de privacidad mediante diseño podría ser una prestación que permita al usuario restringir la captura de imágenes a un cierto perímetro, evitando que la cámara capture imágenes fuera de este perímetro (lo que ocurriría en caso contrario).

El controlador también tiene la obligación de implementar medidas técnicas u organizativas que, por defecto, garantizan el procesamiento menos intrusivo de la privacidad de los datos personales en cuestión, y a ello se refiere el GDPR como privacidad por defecto. En el contexto de una cámara con firmware, un ejemplo relevante de privacidad por defecto podría ser el de una prestación que haga que el usuario establezca el perímetro exacto de captura de la imagen siguiendo el ejemplo anterior.

El derecho de los individuos
Uno de los elementos principales que han impulsado el GDPR es la necesidad de ofrecer a los individuos una mayor protección y un conjunto de derechos para controlar sus datos privados. Hay algunos requisitos muy específicos en las cláusulas del reglamento que indican que la parte encargada del procesamiento o almacenamiento de los datos personales debe responsabilizarse del mantenimiento de la privacidad de dicha información.

El reglamento también ofrece a los individuos el derecho de saber cuándo se recopilan los datos en el punto de captura, y cómo se van a usar. En el caso de la videovigilancia, por ejemplo, esto significa que es preciso colocar unas señales apropiadas en la zona donde se esté realizando la videovigilancia.

2. ¿Cómo afecta el GDPR a la videogilancia?

Una gran parte del debate alrededor del GDPR se ha centrado en el almacenamiento y procesamiento seguros de los datos más tradicionales – como listas de nombres y direcciones de email guardadas en una hoja de cálculo o en una base de datos. Pero ha habido un interés mucho menor en las imágenes móviles, aunque éste es un campo al que las compañías deberían prestar más atención.

Siempre que la videovigilancia contenga datos personales, se encontrará sujeta a las disposiciones del GDPR.

Impacto del GDPR en el uso de equipos de vigilancia, como productos y soluciones basados en cámaras
En lo que se refiere a los productos y las soluciones vendidos por Axis, es el usuario, en calidad de controlador del producto o de la solución, el principal responsable de que el uso del producto o de la solución para procesamiento de datos personales cumpla con el GDPR. Esto significa que, dentro del contexto de los productos y de las soluciones, el cumplimiento o las infracciones del GDPR dependen del uso por parte del usuario del producto o de la solución.

Impacto del GDPR en el uso de servicios específicos alojados
En el caso de los servicios, el cumplimiento del GDPR depende en cierta medida del suministro de dichos servicios, que es responsabilidad de Axis. Pero, así y todo, el cumplimiento o las infracciones del GDPR dependen del uso del servicio por parte de los clientes. Debemos examinar en cada aplicación del tipo de obligaciones relacionadas con el GDPR que puedan surgir y quién tiene dichas obligaciones.

Tomemos como ejemplo un servicio alojado, como el AXIS Guardian. Así es como se aplica habitualmente el GDPR y quién se responsabiliza de ello:

> Clientes de un operador de alarmas: el controlador de los datos personales contenidos en el vídeo capturado por el sistema de videovigilancia del usuario y que se carga en el AXIS Guardian.
> Operador de alarmas: El procesador de los datos en nombre de los usuarios de los datos personales cargados en el AXIS Guardian por el usuario (por ejemplo, la información y los vídeos capturados de los empleados del usuario).
> Axis: el procesador de los datos en nombre del operador de alarmas para los datos personales cargados en el AXIS Guardian por el operador de la alarma (por ejemplo, la información de los empleados del operador de alarmas) y el subprocesador de datos personales en nombre del operador de alarmas para los datos personales cargados en el AXIS Guardian por los clientes del operador de la alarma (vídeo capturado).
> Amazon Web Services: El subprocesador de datos en nombre de Axis para los datos personales cargados en el AXIS Guardian por el operador de alarma s y por los clientes del operador de alarma s (usuarios).

2.1 Pasos hacia el cumplimiento de GDPR

El GDPR es un reglamento que va a afectar al procesamiento de los datos por parte de las compañías - incluyendo los datos de vídeo- en el futuro.

Como mínimo, cada organización que procese datos personales necesitará una o más personas especializadas responsables del procesamiento de esta información cumpliendo con el GDPR y con las políticas establecidas por la compañía y el número de horas de personal dedicadas a esta tarea dependerá del tamaño de la organización y de la cantidad de datos personales recopilados y procesados). Asimismo, para algunas organizaciones, el GDPR requerirá el nombramiento de un Director de Protección de Datos (DPO) encargado de estas tareas.

También vamos a observar cambios en los procesos administrativos. Con el GDPR, las organizaciones necesitan mantener unos registros detallados y precisos de sus actividades de procesamiento. Existen varias informaciones que se necesitan registrar, incluyendo (aunque sin limitarse a ello) las siguientes:

> La categoría a la que pertenecen los datos personales procesados (clientes, empleados, visitantes de la tienda, etc.)
> los fines para los que se usan los datos personales
> Si los datos personales van a ser transferidos – a otras compañías y/o fuera de la UE)
> El tiempo que se van a almacenar los datos personales
> Las medidas tomadas por la organizaciónen relación a cada actividad independiente para el procesamiento de datos, con el objetivo de garantizar el cumplimiento del GDPR

Todo esto es relevante cuando hablamos del almacenaje de imágenes de videovigilancia.

Las organizaciones están obligadas a explicar por qué una cámara de vídeo se encuentra instalada en un lugar determinado, lo que se graba y por qué se graba. En el caso de la videovigilancia, se deberían proporcionar unas señales específicas en donde se utilice la videovigilancia para informar sobre estas actividades.

El controlador de los datos se puede ver obligado a realizar una Valoración del Impacto de la Protección de Datos (DPIA) a la hora de instalar una cámara en un lugar público. Una DPIA debería incluir (las características exactas de una DPIA se deben decidir para cada caso):

> Una descripción sistemática de las operaciones de procesamiento planificadas en lo que a los fines se refiere
> Una valoración de la necesidad y la proporcionalidad de las operaciones de procesamiento y sus objetivos
> la valoración de los derechos y de las libertades de los individuos
> Las medidas planificadas para ocuparnos de estos riesgos, incluyendo las protecciones y los mecanismos para garantizar la protección de los datos personales y el cumplimiento del GDPR (teniendo en cuenta los derechos y los intereses legítimos de los individuos y de otras personas afectadas)

Una de las principales características del nuevo reglamento es que las personas que estén siendo monitorizadas necesitan estar informadas de los datos que se están recopilando y del uso de dicha información.

El reglamento establece algunas reglas básicas claras sobre el cifrado y sobre la protección de los datos. El hecho de que los datos se encuentren capturados en vídeo no altera estas obligaciones.

Por lo tanto, las empresas que almacenan vídeo tienen unas responsabilidades muy claras en el apartado de conservación de datos personales y deben introducir medidas de gran calado para evitar el acceso sin autorización. En este sentido, es importante poner por escrito quién tendrá acceso a las cámaras y a las grabaciones.

Las organizaciones deben disponer también de un procedimiento para los casos en que una persona decida ejercer el derecho de acceso a sus datos personales o solicitar su eliminación. Este procedimiento

les permitirá cumplir con la obligación de dar respuesta a estas solicitudes en el plazo de un mes, según lo estipulado por el GDPR. Cuando se recibe una solicitud de este tipo, es razonable esperar que el solicitante proporcione la información necesaria para localizar sus datos, por ejemplo un marco temporal aproximado y el sitio donde se realizaron las grabaciones.

Las empresas deben introducir medidas de gran calado para evitar el acceso sin autorización a los datos personales que guardan. Las estrategias utilizadas por cada empresa variarán en función de los desafíos a los que se enfrenta. Sin embargo, hay algunos requisitos comunes a todas ellas: usar potentes controles de seguridad, estar al día en materia de buenas prácticas de ciberseguridad y trabajar con socios de confianza capaces de ofrecer soluciones de hardware, software y posventa con una seguridad de primer nivel.

3. Conclusión

En última instancia, el usuario del equipo de vigilancia, las soluciones de vigilancia y los servicios de vigilancia es el responsable de cumplir el GDPR y de proteger los derechos de las personas cuyos datos personales son objeto del tratamiento. Las organizaciones que han hecho poco o nada en este terreno deberán ponerse manos a la obra. En cambio, las empresas que han hecho los deberes y han prestado atención a las responsabilidades que deberán asumir según el reglamento lo tienen más fácil.

Como usuario de equipos de vigilancia, soluciones de vigilancia y servicios de vigilancia, es importante que trabaje con proveedores y distribuidores con un compromiso inequívoco con el respeto y la protección de la privacidad y los datos personales de las personas. Como usuario de equipos de vigilancia, soluciones de vigilancia y servicios de vigilancia, debe poder contar con el apoyo y la asistencia técnica de sus proveedores y distribuidores para dar cumplimiento al GDPR.

Recursos adicionales:

Texto completo del GDPR

Sitio web del Supervisor Europeo de Protección de Datos

Sitio web de pautas de protección de datos para pequeñas y medianas empresas

72049/ES/R1/1807

Axis Communications in perspective

Axis trabaja para un mundo más eficiente y seguro diseñando soluciones en red que aportan información para mejorar la seguridad y abrir la puerta a nuevas formas de trabajar. Axis, líder en soluciones de vídeo en red, ofrece productos y servicios de videovigilancia, control de acceso y sistemas de audio, así como analítica de vídeo.

Axis cuenta con más de 2.800 empleados propios en más de 50 países y colabora con empresas de todo el mundo para hacer llegar sus soluciones a los clientes. Fundada en 1984, Axis es una empresa sueca que cotiza en el índice NASDAQ de la bolsa de Estocolmo con el código AXIS.

Para más información sobre Axis, visite nuestra web www.axis.com.

AXIS COMMUNICATIONS