



Guía del Reglamento General de Protección de Datos y el Video Inteligente



Introducción

En los últimos años, la protección de datos, la privacidad y la ciberseguridad han pasado de ser actividades entre bastidores a noticias de primera plana, surgiendo como una prioridad estratégica para las empresas que manejan datos personales de clientes. De manera que las violaciones de datos personales y los crímenes cibernéticos aumentan en número y magnitud, los gobiernos están interviniendo para establecer y asegurar el cumplimiento de las normas que los 'recolectores' y 'procesadores' de datos deben seguir para operar su negocio. Aunque desde hace mucho tiempo la tecnología desarrollada para la videovigilancia ha estado sujeta a restricciones de retención y privacidad de datos en ciertos países y regiones, los requisitos han variado mucho.

La legislación más reciente y completa que aborda la protección de datos y la privacidad es el [Reglamento General de Protección de Datos](#) (GDPR, por sus siglas en inglés) de la Unión Europea, que entró en vigor el 25 de mayo de 2018. Aunque la Unión Europea (UE) es quien está impulsando este reglamento, su impacto va más allá, porque aplica a cualquier organización que recopile o procese datos personales de un residente de la UE, independientemente de la ubicación de esa organización.

Cuando se aplica al video, los datos personales son cualquier información que sirva para identificar de forma única a un individuo.

El GDPR y la Videovigilancia

El GDPR define como datos personales cualquier información relacionada con un individuo identificado o identificable, como sería su nombre, domicilio, dirección de correo electrónico, datos bancarios, publicaciones en sitios de redes sociales o dirección IP de la computadora, entre otros. Los datos personales también incluyen información recopilada mediante las aplicaciones de punto de venta (POS) o las basadas en analítica, tal como el software de reconocimiento facial o de matrícula, con algunas excepciones. Cuando se aplica a la videovigilancia, los datos personales son básicamente cualquier información que sirva para identificar de forma única a un individuo.

Para conocer más, puede leer el artículo [Entendiendo el GDPR y su impacto en la seguridad por video](#) de Peter Strom, presidente y director general de March Networks.

Cabe destacar que, aunque el GDPR exige que los datos de video estén protegidos, no describe exactamente cómo debe hacerse. La normativa se enfoca en los mandatos en torno a la privacidad y la protección de datos que necesitan ser aplicables por igual en la actualidad como en los años venideros, por lo tanto, no incluye los requisitos detallados o las listas de comprobación para las tecnologías disponibles actualmente, incluidas las de video. Como consecuencia, no hay una definición exacta de lo que constituiría la conformidad de los datos de video y son diversas las interpretaciones. Del mismo modo, ningún organismo ha sido acreditado bajo el reglamento* para certificar las soluciones de video con el "Sello Europeo de Protección de Datos".

*Hasta mayo 2018

Cómo Apoyan las Soluciones de March Networks el GDPR

Como proveedor global de soluciones de video inteligentes, March Networks ha seguido los requisitos del GDPR muy de cerca. A principios de 2017, contratamos a un consultor externo de privacidad de datos de la UE para que realizara una auditoría independiente sobre nuestra gama de productos frente a las normativas para la videovigilancia del reglamento.

Como era de esperarse, muchas características ya incorporadas en nuestros productos para ayudar a nuestros clientes a cumplir con las regulaciones existentes, incluyendo la directiva anterior de protección de datos [95/46/CE](#) de la UE, son aplicables al GDPR. Entre éstas están las siguientes:

Características de Autenticación que permiten a los clientes ejercer un estricto control y restringir quién tiene acceso al video grabado. Debido a que nuestros sistemas de nivel empresarial soportan grandes despliegues con cientos o miles de usuarios, incorporamos características que ayudan a salvaguardar los datos, incluyendo: derechos de acceso totalmente configurables (hasta el nivel de cámara específica); verificación de acceso opcional mediante tarjeta inteligente con claves de cifrado asimétrico; registros de auditoría y capacidad de generación de informes; e integración con LDAP para que pueda aplicarse toda la información de la cuenta de usuario (p. ej. niveles de privilegio, contraseñas y dominios) directamente del directorio de la red corporativa de la organización, si así se desea.

Características de Anonimato que dejan a los clientes aplicar máscaras de privacidad fijas para ocultar la identidad de los individuos capturados involuntariamente por el sistema de videovigilancia, como sería el caso de alguien que camina por la acera afuera de un banco o una tienda o bien, las matrículas de los coches que van junto a un autobús de transporte público. Los sistemas de March Networks soportan máscaras de privacidad configurables que permanecen intactas tanto en el video en vivo como en el grabado, asegurando que los clientes puedan evitar de forma eficaz la recopilación y el almacenamiento de estos datos identificables. [Vea cómo funciona nuestra función de enmascaramiento.](#)

Características de Encriptación y Antimanipulación para garantizar a los clientes que la información en video que están recopilando se transporta por la red de manera segura. Nuestros sistemas usan TLS 1.2, un protocolo estándar de la industria diseñado para proteger la privacidad de la información sobre la red. Además, aplicamos un algoritmo de control seguro (SHA-256) al video exportado, lo que proporciona una función antimanipulación para impedir que se autentique cualquier video exportado que haya sido modificado.

Características de Retención que pueden configurarse para borrar automáticamente el video después del periodo de tiempo máximo de retención. Nuestros sistemas también les permiten a los usuarios autorizados borrar manualmente una parte seleccionada del archivo de video. Aunque el GDPR no establece límites específicos del tiempo que una organización puede archivar su video de vigilancia, sí menciona que la información no debe almacenarse por más tiempo que el necesario para el 'fin inicial' definido, pero aquí la flexibilidad es importante, dados los diferentes requisitos del cliente o del país.

Características de Transmisión de Video, incluyendo soporte para múltiples secuencias de video y cada una con resoluciones configurables. Aunque el GDPR no especifica una resolución fija de la imagen de video, la misma restricción que exige a las organizaciones limitar el procesamiento de datos a no más del 'fin inicial' definido, aplica aquí. Con la capacidad de múltiples secuencias de video, los clientes tienen la flexibilidad de personalizar las diferentes transmisiones y resoluciones de video para cumplir con sus aplicaciones específicas.



Diseñar soluciones seguras de protección de datos es parte del ADN de March Networks, que se remonta a nuestras profundas raíces en tecnologías de la información y redes.

Como parte de la auditoría que llevamos a cabo, también identificamos áreas donde consideramos que sería beneficioso contar con mayor funcionalidad. Por lo tanto, incorporamos esas características en nuestra línea de productos y ahora confiamos en nuestra capacidad para apoyar a nuestros clientes y asegurar que están bien preparados para cumplir con la legislación del GDPR.

Además, seguimos incorporando nuevas características orientadas a la privacidad en nuestra línea de productos, tales como las capacidades para reforzar la gestión de contraseñas y la configuración de los derechos de usuario. Si bien estas capacidades van más allá de lo que puede considerarse legislado por el GDPR, reflejan la dedicación de March Networks para ofrecer soluciones seguras que faciliten a las organizaciones el logro de sus objetivos y el cumplimiento de los requisitos de seguridad y privacidad existentes y emergentes.

Un Enfoque Integral sobre la Privacidad de Datos y la Ciberseguridad

March Networks siempre ha estado comprometido a proveer productos seguros para la videovigilancia y la inteligencia de negocios basada en video a las organizaciones. Hemos ofrecido por más de 15 años soluciones de clase empresarial a los principales clientes del sector financiero, minorista y comercial del mundo y seguido los principios de privacidad por diseño que guían cómo nuestras soluciones capturan, integran y almacenan el video y la información del negocio. Desde

el lanzamiento de nuestra primera Integración de Transacciones Financieras y de Comercios (FTI/RTI, por sus siglas en inglés) hace una década, hemos trabajado estrechamente con nuestros clientes, socios y expertos en privacidad para comprender y abordar los diferentes requisitos de privacidad de datos en todo el mundo.

Diseñar soluciones seguras de protección de datos es parte del ADN de March Networks, que se remonta a nuestras profundas raíces en tecnologías de la información y redes. Nuestro enfoque holístico sobre la ciberseguridad implica una visión de 360° de todos los aspectos de nuestro negocio, abarcando nuestros productos, la gente que los construye y los procesos que nos guían. Nuestra compañía ha participado en auditorías exhaustivas de seguridad de clientes Fortune 500 que han examinado todo, desde la seguridad de nuestro Centro de Operaciones de Red hasta cómo controlamos y protegemos nuestro código de software.

También trabajamos con un grupo de integradores de sistemas con mucha experiencia, al que hemos dotado con la información y las herramientas necesarias para asegurar que los sistemas de video de nuestros clientes están bien protegidos. March Networks fue el primero en la industria en introducir una herramienta especialmente diseñada de [auditoría de seguridad móvil](#) en nuestra aplicación GURU para teléfonos inteligentes. Y uno de los primeros en crear un programa proactivo y transparente de [Actualizaciones y Noticias sobre Seguridad](#), que mantiene informados

a los socios y clientes sobre las vulnerabilidades potenciales de seguridad vía alertas por correo electrónico y en nuestra página de Internet. Más recientemente, hemos alcanzado la certificación de Cyber Essentials, reconociéndonos como una empresa cibersegura.



Seguridad y Protección de Datos de March Networks

Un Enfoque de 360°

March Networks está comprometido a ayudar a sus clientes a entender y abordar el GDPR en referencia a la videovigilancia e inteligencia de negocios basada en video, así como a ofrecer productos y soluciones desarrolladas con un enfoque completo que aborde la seguridad cibernética.

Personas

- Profundo patrimonio en tecnologías de la información y redes
- Verificación de antecedentes de los desarrolladores de código que trabajan en el Centro Canadiense de Excelencia de I+D de la compañía
- Seguro Centro de Operaciones de Red (NOC) con acceso restringido
- Oficinas corporativas y laboratorios I+D protegidos con tarjeta de acceso



Procesos

- Seguir los principios de seguridad mediante el diseño en el desarrollo de nuestros productos y sistemas de negocios
- Participar en auditorías exhaustivas de seguridad con clientes Fortune 500
- Operar un amplio programa de Actualizaciones y Noticias sobre Seguridad; proactivo, transparente y disponible a todos los clientes y socios a través de nuestra página de Internet
- Realizar anualmente pruebas de intrusión a los sistemas internos empresariales
- Cyber Essentials de Canadá certificó y nombró a March Networks como una empresa cibersegura

Productos

- Extensa lista de características y capacidades de producto para soportar la autenticación, anonimato, encriptación y antimanipulación del video, retención flexible, transmisión de video múltiple y resolución configurable
- Soluciones que ya cumplen con la directiva anterior de protección de datos 95/46/CE de la Unión Europea
- Herramienta Interactiva de Auditoría de Seguridad a través de nuestra aplicación gratuita GURU para teléfonos inteligentes
- Guía de seguridad de producto

¿Tiene Preguntas? Póngase en contacto con nosotros

Si tiene preguntas adicionales sobre cualquiera de nuestros productos, por favor póngase en contacto con su representante de ventas de March Networks, llamando al +1 613 591 8181 o enviando un correo electrónico a info@marchnetworks.com.

Norteamérica 1 800 563 5564
Latinoamérica +5255 5259 9511
Europa +39 0362 17935
Asia +65 6818 0963
Australia y Nueva Zelanda +61 1300 089 419
Medio Oriente y África +971 4 399 5525

© 2018. March Networks, una compañía de Infinova. Todos los derechos reservados. La información contenida en este documento está sujeta a modificaciones sin previo aviso. MARCH NETWORKS, March Networks Command, March Networks Searchlight, March Networks RideSafe, Shadow Archive y el logotipo de MARCH NETWORKS son marcas comerciales de March Networks Corporation. Infinova es una marca registrada de Infinova Corporation. Todas las demás marcas comerciales son propiedad de sus respectivos dueños. 060-3348-SP-A marchnetworks.com


An Infinova Company