MAKE THE
WORLD SEE

Milestone Systems

Guía de privacidad de acuerdo con el RGPD

milestone

Historial de la versión

Versión del documento	Release	Comentarios
Versión 3	2021 R2	Las actualizaciones de esta versión incluyen: • Garantías contra el funcionamiento de una VPN en modo dividido añadidas a Garantías adicionales en la página 58.
Versión 2	2021 R1	Las actualizaciones de esta versión incluyen: • El tipo de usuario básico está ahora cubierto por el Sello Europeo de Privacidad (Anexo: El sistema Milestone XProtect VMS y el RGPD en la página 54) y (Anexo: Procesamiento de datos en el entorno de Milestone XProtect VMS en la página 63). • Recomendaciones añadidas a Utilizar fondos geográficos en XProtect Smart Client en la página 57. • Recopilación de datos descrita en Integraciones de socios registrados en la página 57. • Registro de autenticación descrito en Datos personales del sistema en la página 64.
Versión 1	2020 R3	Esta es la primera versión de este documento.

Contenido

Historial de la versión **2**

Copyright, marcas comerciales y exención de responsabilidad **5**

Cumplimiento del RGPD y Milestone XProtect VMS **6**

¿Qué es el RGPD? 6

¿Quiénes son los principales interesados en el RGPD en relación con la videovigilancia? **9**

Titular de los datos 9

Derechos de los titulares de los datos 9

Solicitud del titular de los datos 11

¿Qué son los datos personales? 11

Controlador de datos 14

Responsable de seguridad (supervisor del VMS) 16

Administración de los derechos de los usuarios 16

Formación en protección de datos 18

Administrador del sistema VMS 18

Operador de VMS 19

Gestión de datos exportados 19

Tratamiento de los datos exportados en las notificaciones y el correo electrónico 21

Violación de información personal 22

Encargado del tratamiento 23

Resumen **24**

Para obtener más información 25

Anexos **27**

Anexo: Cumplimiento del RGPD 27

¿Tiene una base legal para recopilar datos? 27

Realización de una evaluación de impacto 32

Derechos individuales 33

Derecho de acceso 34

Derecho al olvido (Derecho a la supresión) 36

Derecho a la limitación del tratamiento 38
Privacidad por diseño 38
¿Qué debe hacer? 39
Requisitos para la privacidad por diseño 39
Privacidad por diseño y privacidad por defecto 40
Instalación y configuración del sistema de videovigilancia 42
¿Quién debe tener acceso al VMS? 44
Protección de los datos almacenados y transmitidos 45
Responsabilidad 46
Lista de comprobación para asegurar la integridad y la confidencialidad 47
Anexo: Aviso en el lugar 48
Anexo: Política de videovigilancia 49
Anexo: Evaluación del impacto de la protección de datos 50
Riesgos inherentes al uso del VMS 52
Anexo: Acuerdo de procesamiento de datos 54
Anexo: El sistema Milestone XProtect VMS y el RGPD 54
Garantías adicionales 58
Anexo: Procesamiento de datos en el entorno de Milestone XProtect VMS 63

Copyright, marcas comerciales y exención de responsabilidad

Marcas comerciales

XProtect es una marca comercial registrada de Milestone Systems A/S.

Microsoft y Windows son marcas comerciales registradas de Microsoft Corporation. App Store es una marca de servicios de Apple Inc. Android es una marca registrada de Google Inc.

Todas las demás marcas comerciales de este documento pertenecen a sus respectivos propietarios.

Limitación de responsabilidad

Este documento está únicamente concebido como información general, y se ha elaborado con la debida diligencia.

Cualquier daño que pueda derivarse del uso de esta información será responsabilidad del destinatario, y nada de lo aquí escrito podrá ser considerado como ningún tipo de garantía.

Milestone Systems A/S se reserva el derecho de hacer modificaciones sin notificación previa.

Todos los nombres de personas y organizaciones utilizados en los ejemplos de este documento son ficticios. Todo parecido con cualquier persona física, en vida o fallecida, o jurídica real es pura coincidencia y carece de intencionalidad alguna.

Este producto podrá hacer uso de software de terceros, respecto del cual es posible que sean de aplicación condiciones propias. Si ese es el caso, encontrará más información en el archivo 3rd_party_software_terms_and_conditions.txt, que se encuentra en la carpeta de instalación de su sistema Milestone.

Cumplimiento del RGPD y Milestone XProtect VMS

El 25 de mayo de 2018 entró en vigor el Reglamento General de Protección de Datos (RGPD) europeo. El objetivo de este reglamento es dar a las personas un mayor control sobre cómo se recopilan, procesan y comparten sus datos personales.

El RGPD proporciona una estructura a las empresas que aclara sus funciones y responsabilidades y da a las personas la oportunidad de controlar cómo se utilizan sus datos personales.

Este documento le proporciona una visión general de los requisitos y de cómo puede trabajar con el cumplimiento del RGPD cuando utilice el sistema de gestión de vídeo (VMS) de XProtect.

Consulte Anexo: El sistema Milestone XProtect VMS y el RGPD en la página 54 para obtener información específica sobre la mejor manera de hacer que un sistema Milestone XProtect VMS cumpla con el RGPD.

Limitación de responsabilidad: La información incluida en este documento y las posibles recomendaciones se facilitan tal cual. Seguir este documento no significa implícitamente que su sistema cumpla con el RGPD.

El Milestone XProtect VMS requiere configuración. Cualquier configuración o modificación de los ajustes debe cumplir con la ley de protección de datos de la UE. Si bien la Anexo: El sistema Milestone XProtect VMS y el RGPD en la página 54 y Garantías adicionales en la página 58 proporcionan información sobre cómo iniciar una configuración válida, debe respetar las leyes de protección de datos de la UE cuando siga configurando el sistema.

¿Qué es el RGPD?

El Reglamento General de Protección de Datos (RGPD) es un conjunto de normas que regulan todas las formas de datos personales que posee una organización. El RGPD otorga a cada individuo la propiedad de sus datos personales y, por el lado de la organización, introduce la responsabilidad en todas las etapas del tratamiento y del almacenamiento de datos. El RGPD lo hace proporcionando una serie de derechos a los individuos y estableciendo las correspondientes obligaciones a las organizaciones que procesan datos personales.

El RGPD armoniza las leyes de privacidad de datos en toda la UE, y complementa las normativas nacionales existentes en materia de videovigilancia y CCTV.

A pesar de que el RGPD es una normativa de la UE, afecta a muchas otras partes del mundo.
Es aplicable al tratamiento de datos personales por parte de un responsable o un encargado del tratamiento en la Unión Europea, independientemente de que el tratamiento tenga lugar en la Unión Europea o no.
Es aplicable al tratamiento de datos personales por parte de un responsable o encargado del tratamiento no establecido en la Unión Europea, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a los titulares de los datos en la Unión Europea; o el seguimiento de su comportamiento en la medida en que éste tenga lugar en la Unión Europea.
Además, muchas otras partes del mundo están aplicando normas de protección de la privacidad similares, basadas en los principios básicos del RGPD.

El RGPD se impone a través de las autoridades nacionales.

En caso de infracciones, las multas son elevadas:

- Hasta el 4% de los beneficios anuales de la empresa en todo el mundo
- Hasta 20 millones de Euros por incidente

¿Quién es el responsable de garantizar que un sistema de gestión de vídeo XProtect en funcionamiento cumpla con el RGPD?

El propietario del VMS es responsable de cumplir con el reglamento del RGPD, incluido:

- Instalaciones reales y el uso aplicado
- Procesos organizativos y madurez
- Notificación de violaciones de datos y comunicación a las autoridades

El RGPD no se aplica a ningún producto específico, pero la combinación del producto, los datos que procesa y el uso del producto y los datos afectan al cumplimiento del RGPD.

El RGPD tiene implicaciones directas para los instaladores, integradores de sistemas y usuarios de la tecnología de videovigilancia.

El propietario del VMS es el responsable del tratamiento de los datos (consulte Controlador de datos en la página 14).

El responsable del tratamiento de datos puede subcontratar parte o la totalidad de las operaciones del VMS a un procesador de datos, por ejemplo, una empresa de seguridad. Si este es el caso, el responsable del tratamiento de datos y el procesador de datos del mismo deberán disponer de un *acuerdo de procesamiento de datos*. El *Acuerdo de procesamiento de datos* establece qué datos se procesan, cómo se protegen y cuánto tiempo se conservan los datos (consulte Encargado del tratamiento en la página 23 y Anexo: Acuerdo de procesamiento de datos en la página 54).

¿Todas las instalaciones de videovigilancia están obligadas a cumplir con el RGPD?

El RGPD es aplicable a los responsables del tratamiento y a los procesadores dentro de la Unión Europea, independientemente del lugar donde se procese el vídeo.

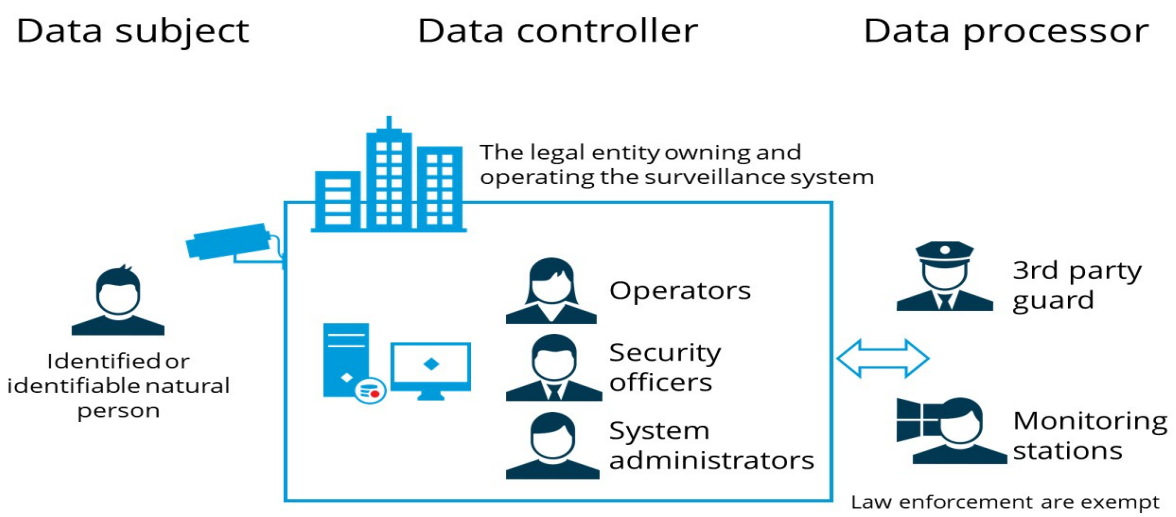
Además, el RGPD protege la privacidad de cualquier residente del área geográfica de la UE, cubre todas las formas de videovigilancia dentro de la UE y protege a los ciudadanos de todos los países que residen en la UE (artículo 3, RGPD).

Para obtener más información sobre el RGPD, especialmente en relación con la videovigilancia, consulte Anexo: Cumplimiento del RGPD en la página 27.

¿Quiénes son los principales interesados en el RGPD en relación con la videovigilancia?

Cuando se trata del RGPD y la videovigilancia, hay tres clases de interesados. Esta sección del documento define a cada una de las partes interesadas y describe sus respectivas responsabilidades en relación con el RGPD.

- Titular de los datos en la página 9
- Controlador de datos en la página 14
- Encargado del tratamiento en la página 23



Titular de los datos

Un titular de datos es cualquier persona cuyos datos personales se recogen, conservan o tratan.

Los titulares de los datos son los objetos vistos de la videovigilancia, ya sea intencionada o involuntaria.

Los sujetos de datos son también cualquier persona registrada que participe en el funcionamiento del VMS, por ejemplo, los operadores o los guardias de terceros nombrados.

El objetivo principal del RGPD es proteger los datos personales de estos titulares.

Derechos de los titulares de los datos

Los artículos 12 a 23 del RGPD cubren los derechos del titular de datos.

- Sección 1: Transparencia y modalidades
  - Artículo 12: Información, comunicación y modalidades transparentes para el ejercicio de los derechos del titular de los datos
- Sección 2: Información y acceso para los datos personales
  - Artículo 13: Información que debe facilitarse cuando se recojan datos personales del titular de los datos
  - Artículo 14: Información que debe facilitarse cuando los datos personales no se hayan obtenido del titular de los datos
  - Artículo 15: Derecho de acceso del titular de los datos (consulte Derecho de acceso en la página 34)
- Sección 3: Rectificación y eliminación
  - Artículo 16: Derecho de rectificación
  - Artículo 17: Derecho al olvido (Derecho a la supresión) (consulte Derecho al olvido (Derecho a la supresión) en la página 36)
  - Artículo 18: Derecho a la limitación del tratamiento (consulteDerecho a la limitación del tratamiento en la página 38)
  - Artículo 19: Obligación de notificar la rectificación o supresión de los datos personales o la limitación del tratamiento
  - Artículo 20: Derecho a la portabilidad de los datos
- Sección 4: Derecho de oposición y toma de decisión individual automatizada
  - Artículo 21: Derecho de oposición
  - Artículo 22: Toma de decisión individual automatizada, incluida la elaboración de perfiles
- Sección 5: Restricciones
  - Artículo 23: Restricciones

De ellos, los derechos más relevantes en el contexto de la videovigilancia son:

El derecho a la información (artículos 12 a 14 y 34, RGPD)	El artículo 12 trata de la transparencia y las modalidades, mientras que los artículos 13 y 14 tratan sobre la información y el acceso a los datos personales. Estos artículos ofrecen al titular de los datos la posibilidad de recibir información sobre qué datos personales se recogen y durante cuánto tiempo se conservan. En el contexto del VMS, consulte Anexo: Aviso en el lugar en la página 48. El artículo 34 proporciona al titular de los datos el derecho a recibir información en caso de que se produzca una violación de los datos si ésta puede suponer un alto riesgo para los derechos y libertades del titular.

El derecho de acceso (Artículo 15, RGPD)	Este derecho proporciona al titular de los datos la posibilidad de acceder a sus datos personales que están siendo procesados, por ejemplo, grabaciones de vídeo del titular. El titular de los datos tiene derecho a solicitar a una empresa información sobre qué datos personales (sobre él o ella) se están procesando y la justificación de dicho tratamiento.
El derecho a la supresión ("derecho al olvido") (Artículo 17, RGPD)	Este derecho proporciona al titular de los datos la posibilidad de solicitar la supresión de sus datos. En el contexto del VMS, la supresión a petición de los interesados es excepcional debido a los intereses del responsable del tratamiento y a los breves plazos de conservación. (Consulte Anexo: Política de videovigilancia en la página 49 y *Eliminar parcialmente grabaciones de vídeo* en Anexo: El sistema Milestone XProtect VMS y el RGPD en la página 54).
El derecho de oposición (Artículo 21, RGPD)	Este derecho proporciona al titular de los datos la posibilidad de oponerse al tratamiento de sus datos personales. En el contexto del VMS, otros intereses, como los intereses legítimos (detección de fraudes, salud y seguridad), las obligaciones legales (contabilidad, lavado de dinero) o incluso el cumplimiento contractual (contratos de trabajo), pueden prevalecer sobre los intereses y derechos del titular de los datos. En todos los casos, esto debe ser totalmente transparente para que el titular de los datos pueda conocerlo y oponerse. Si el titular de los datos se opone, el responsable del tratamiento debe valorar la objeción o, de lo contrario, podría enfrentarse a una multa.

Solicitud del titular de los datos

Su empresa debe tener un proceso para gestionar las solicitudes de derechos de los titulares de los datos, por ejemplo, aplicar el derecho de solicitud de acceso. Dicha solicitud debe gestionarse en un plazo razonable. Según el artículo 12 (3) del RGPD, esto es "sin demora indebida y, en cualquier caso, dentro de un mes a partir de la recepción de la solicitud." Se recomienda utilizar una plantilla de *solicitud del titular de los datos* para documentar dichas solicitudes, ya que puede ser vital en un caso del RGPD con las autoridades nacionales de protección de datos. Para ver un modelo de solicitud del titular de los datos, consulte la plantilla *Milestone Solicitud del titular de los datos*.

La política de videovigilancia describe la solicitud del titular de los datos (consulte Anexo: Política de videovigilancia en la página 49).

¿Qué son los datos personales?

Para cumplir con el RGPD, debe saber qué son los datos personales y limitar la recopilación de esos datos solo a lo necesario.

Según el reglamento, la información personal es cualquier información relativa a una persona identificada o identificable.

Una persona identificable es alguien que puede ser identificado directa o indirectamente, por referencia a un identificador como:

- Un nombre
- Un número de identificación
- Dato de localización
- Identificador en línea, como direcciones IP o identificador de cookies
- Datos de usuario
- Imágenes de vídeo
- O para uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona

La información personal es cualquier tipo de información que pueda utilizarse directa o indirectamente para identificar a una persona física (titular de los datos). Estos son los datos que pueden utilizarse para identificar los objetos vistos de la videovigilancia, tanto si se recogen intencionada como accidentalmente.

Los datos personales que están protegidos por el RGPD son:

- Datos que son procesados por el producto de TI o el servicio basado en TI (por ejemplo, nombre y dirección de una persona, imagen de vídeo, datos de pago, datos sanitarios).
- Datos que se producen incidentalmente cuando se utiliza el producto o servicio (por ejemplo, datos de uso, archivos de registro, datos estadísticos, datos para la autorización, datos de configuración). Estos datos pueden ser información personal de los usuarios del servicio, datos personales de las personas que administran el producto o servicio (esto puede incluir tanto al personal del proveedor de servicios como al personal de los usuarios del producto o servicio), o datos de configuración relevantes para la privacidad (consulteControlador de datos en la página 14).

La información personal se define como cualquier información relativa a una persona física identificada o identificable o a un titular de datos, por ejemplo:

• Nombre completo • Dirección del domicilio • Dirección de correo electrónico • Número de teléfono • Dato de localización • Identidad digital	• Matrícula del vehículo • Número del permiso de conducir • Números de tarjetas de crédito • Información identificable, imágenes, etc., como grabaciones de vídeo e imágenes fijas • Actividades de los usuarios, como las que se encuentran en los archivos de registro

Esta información no es necesariamente sólo una relación directa con el objeto. La información personal también puede ser un cuasi-identificador. Los cuasi-identificadores son piezas de información que no son de por sí identificadores únicos, pero que están lo suficientemente bien correlacionados con algo como para que puedan combinarse con otros cuasi-identificadores para crear un identificador único. Los cuasi-identificadores son particularmente importantes cuando se trata de categorías especiales de datos personales.

Las categorías especiales de datos personales incluyen los datos que describen el origen racial y étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical, los datos genéticos, los datos biométricos, los datos relativos a la salud o los datos relativos a la vida sexual o la orientación sexual, por ejemplo:

• Historial médico • Datos biométricos (incluidos fotos, vídeos y huellas dactilares) • Antecedentes penales • Identidad racial o étnica	• Información genética • Opiniones políticas y compromisos • Creencias religiosas o filosóficas • Orientación sexual e historial

Esta es la información personal que potencialmente recoge un sistema de videovigilancia:

¿Qué tipos de descripciones de datos personales, almacenados por XProtect, están incluidos en el ámbito de aplicación del RGPD?

La información personal es cualquier tipo de información que pueda utilizarse directa o indirectamente para identificar a una persona física (titular de los datos). Puede tratarse de flujos de videovigilancia, de una sola imagen o de una secuencia de vídeo combinada con información de localización procedente de cámaras y/o mapas en capas, de una integración de control de acceso que identifique una tarjeta de acceso personal y la combine con una localización específica, o de datos procedentes del reconocimiento de matrículas (LPR) con o sin datos de localización.

Las categorías especiales de información personal se dan cuando la videovigilancia está cerca de hospitales (relacionada con información sanitaria), cárceles (condenas penales), actividad política (afiliación sindical), actividad religiosa o imágenes que revelan la orientación sexual (por ejemplo, bares gays).

Los datos personales también se refieren a los datos de los usuarios (operador, supervisor y administrador) de la actividad y el registro de auditoría. Esto incluye los registros personales de los usuarios de XProtect Smart Client, incluidas las marcas de tiempo de inicio y fin de sesión y el registro de auditoría de los flujos de vídeo, audio o metadatos a los que se ha accedido, así como la reproducción y exportación de las grabaciones.

Consulte Riesgos inherentes al uso del VMS en la página 52 para asegurarse de que no se vulneran los derechos personales.

Controlador de datos

En el contexto de la videovigilancia, los controladores de datos son los propietarios y operadores de los sistemas de videovigilancia. Los responsables del tratamiento son la entidad jurídica que recopila, procesa y comparte datos sobre el titular de los mismos.

¿Cuáles son las responsabilidades del responsable del tratamiento de datos?

Los responsables del tratamiento deben respetar los principios de protección de datos y cumplir determinadas obligaciones específicas. El responsable del tratamiento debe aplicar las medidas técnicas y organizativas adecuadas para garantizar y poder demostrar que el tratamiento se realiza de conformidad con el RGPD. Esto también incluye:

- Aplicar y mantener políticas y procedimientos de seguridad de la información para proteger los datos personales. Estas políticas y procesos internos deben ser aprobados al más alto nivel dentro de la organización y, por tanto, ser vinculantes para todos los miembros del personal.
- Mantener una visión general de los registros de datos personales y de los flujos de tratamiento, por ejemplo, el registro de actividades de tratamiento (artículo 30 del RGPD) y una lista de los sistemas y archivos que manejan información personal (el sistema XProtect VMS y otros sistemas que guardan datos personales, como los registros del personal, los acuerdos del procesador de datos, etc., incluyendo información sobre cómo y dónde fluyen los datos personales). Para ver un modelo de registro de actividades de tratamiento, consulte la plantilla de *Milestone Registro de actividades de tratamiento* .

- Poner en marcha mecanismos que ejecuten las políticas y procesos internos, incluidos los procedimientos de reclamación, para que dichas políticas sean efectivas en la práctica. Esto incluye la concienciación sobre la protección de datos y la formación e instrucción del personal. La formación de concienciación está disponible en https://www.milestonesys.com/solutions/services/learning-and-performance/.
- Definición de la política de videovigilancia (consulte Anexo: Política de videovigilancia en la página 49). Esta política debe hacer referencia a las leyes locales relativas a la videovigilancia.
- Llevar a cabo las Evaluaciones de impacto sobre la protección de datos, en particular para determinadas operaciones de tratamiento de datos que se considera que presentan riesgos específicos para los derechos y libertades de los interesados, por ejemplo, en virtud de su naturaleza, su alcance o su finalidad (consulte Anexo: Evaluación del impacto de la protección de datos en la página 50).
- Garantizar la transparencia de estas medidas adoptadas en relación con los titulares de los datos y el público en general. Los requisitos de transparencia contribuyen a la responsabilidad de los responsables del tratamiento de datos (por ejemplo, la publicación de las políticas de privacidad en Internet, la transparencia de los procedimientos internos de reclamación y la publicación en los informes anuales).
- Publicar el aviso de derecho de información al público (consulte Anexo: Aviso en el lugar en la página 48). Este aviso informa a las personas afectadas de la finalidad de la vigilancia, de quién conserva los datos que se recogen (responsable del tratamiento) y de la política de conservación.
- Asignar la responsabilidad de la protección de datos a personas designadas con responsabilidad directa sobre el cumplimiento de las leyes de protección de datos por parte de sus organizaciones. En particular, nombrar al delegado de protección de datos (DPD).

Delegado de protección de datos (DPD)

Toda organización debe contar con un DPD designado o, al menos, con una persona asignada como responsable de la privacidad.

Desde el principio, los planes para instalar o actualizar un sistema de videovigilancia deben ser comunicados al DPD.

El DPD debe ser consultado en todos los casos y de manera oportuna en todas las cuestiones que tengan que ver con la protección de los datos personales que se tratan cuando se presta o utiliza el servicio.

El DPD debe participar en todas las fases de la toma de decisiones.

Las responsabilidades del DPD incluyen:

- Participar en la definición del objetivo empresarial de la videovigilancia, por ejemplo, la prevención de delitos, la detección de fraudes, la verificación de la calidad de los productos o la salud y seguridad públicas, etc.
- Opinar sobre el proyecto de política de videovigilancia de la organización, incluidos sus anexos, (consulte Anexo: Política de videovigilancia en la página 49), y corregir errores y sugerir mejoras
- Colaborar en las comunicaciones con las autoridades nacionales o regionales de protección de datos

- Comprobar los acuerdos con terceros al compartir datos. Es decir, el mantenimiento y la gestión del *Acuerdo de procesamiento de datos* (consulte Anexo: Acuerdo de procesamiento de datos en la página 54)
- Elaborar informes de cumplimiento y realizar auditorías para obtener la certificación de terceros que aprueben las medidas internas adoptadas para garantizar el cumplimiento de la gestión, la protección y la seguridad de la información personal.
- Almacenar y asegurarse de que el Registro de actividades de tratamiento y las Evaluaciones de impacto sobre la protección de datos (consulte Anexo: Evaluación del impacto de la protección de datos en la página 50) se actualizan cada vez que se realizan cambios relevantes de protección de datos en el VMS. Para ver un modelo de registro de actividades de tratamiento, consulte la plantilla de *Milestone Registro de actividades de tratamiento* .

Roles del responsable del tratamiento de datos

Las siguientes secciones describen las responsabilidades de los respectivos responsables del tratamiento de datos:

- Responsable de seguridad (supervisor del VMS) en la página 16
- Administrador del sistema VMS en la página 18
- Operador de VMS en la página 19

Responsable de seguridad (supervisor del VMS)

Los responsables de seguridad o los supervisores son los encargados de velar por el cumplimiento del entorno del RGPD. Los responsables de seguridad deben:

- Definir los derechos de los usuarios (consulte Administración de los derechos de los usuarios en la página 16)
- Imponer la formación de concienciación del personal (consulte Formación en protección de datos en la página 18)
- Ponerse en contacto con el delegado de la protección de datos (DPD) si se sospecha de un incumplimiento del RGPD, por ejemplo, en el caso de una violación de los datos de los materiales de vídeo (consulteAnexo: Cumplimiento del RGPD en la página 27)
- Aplicar y mantener un alto grado de seguridad general. Para obtener más información sobre cómo asegurar sus instalaciones XProtect VMS ontra los ciberataques, consulte la guía para reforzar.

Administración de los derechos de los usuarios

¿Quién debe tener acceso a los recursos del VMS?

Las organizaciones deben:

- Limitar el acceso de los usuarios a un número reducido de personas claramente identificadas en función de su necesidad de conocimiento.
- Mantener registros de auditoría de los accesos y actividades de los usuarios.

Sólo un número reducido de personas, claramente identificadas, podrá acceder a los datos en función de una necesidad estricta de conocimiento. Asegúrese de que los usuarios autorizados sólo pueden acceder a los datos a los que se refieren sus derechos de acceso. Las políticas de acceso deben ser definidas siguiendo el principio de "mínimo privilegio": el derecho de acceso a los usuarios debe ser concedido sólo a aquellos recursos que sean estrictamente necesarios para llevar a cabo sus tareas.

Al compartir un ordenador, Milestone recomienda que los operadores de VMS no compartan la cuenta de acceso a Windows. Cada operador debe tener una cuenta individual.

Además, los operadores de VMS no deben seleccionar recordar su contraseña al iniciar la sesión en el sistema VMS.

Sólo el responsable de seguridad, el administrador del sistema u otros miembros del personal designados específicamente por el responsable de seguridad para este fin deben poder conceder, modificar o anular los derechos de acceso de cualquier persona. Cualquier provisión, alteración o anulación de los derechos de acceso debe hacerse de acuerdo con los criterios establecidos en la política de videovigilancia (consulteAnexo: Política de videovigilancia en la página 49).

Las personas con derechos de acceso deben ser en todo momento personas claramente identificables. Por ejemplo, no se deben asignar nombres de usuario y contraseñas genéricos o comunes a una empresa de seguridad subcontratada que emplee a varias personas para trabajar en la organización.

La política de videovigilancia debe especificar y documentar claramente la arquitectura técnica del sistema de videovigilancia, quién tiene acceso al vídeo de vigilancia y con qué propósito, y en qué consisten esos derechos de acceso. En particular, debe especificar quién tiene derecho a:

• Ver o acceder al vídeo en tiempo real • Operar las cámaras panorámicas, inclinadas y con zoom (PTZ) • Ver o acceder al vídeo grabado	• Exportar grabaciones y registros de auditoría • Eliminar o quitar dispositivos (cámaras) y borrar las grabaciones • Alterar cualquier dato después de la configuración inicial

Además, debe asegurarse de que sólo obtengan estos permisos quienes necesiten acceder a las siguientes funciones del VMS:

• Administrar el VMS • Crear / editar / ver / eliminar marcadores • Crear / editar / ver / eliminar bloqueos de evidencias • Retirar máscaras de privacidad • Exportar a rutas definidas (por ejemplo, sólo exportar el formato con cifrado XProtect a una unidad compartida)	• Leer registros de auditoría • Iniciar/detener grabación • Crear / editar / eliminar / activar / bloquear / liberar valores preestablecidos de PTZ • Crear / editar / eliminar / iniciar / detener esquemas de patrulla PTZ • Permisos de audio, metadatos, E/S y eventos

Formación en protección de datos

Todo el personal con derechos de acceso, incluido el personal subcontratado que lleva a cabo las operaciones cotidianas de CCTV o el mantenimiento del sistema, debe recibir formación en materia de protección de datos y debe conocer a fondo las disposiciones del RGPD en la medida en que sean importantes para sus tareas. La formación debe prestar especial atención a la necesidad de evitar la divulgación del vídeo de vigilancia a cualquier persona que no esté autorizada.

La formación del personal es obligatoria y debe incluir:

- Ciberseguridad
- Exportación de datos VMS

La formación debe realizarse cuando se instala un nuevo sistema, cuando se realizan modificaciones significativas en el sistema, cuando se incorpora una nueva persona a la organización, así como periódicamente después a intervalos regulares. En el caso de sistemas existentes, la formación inicial debe realizarse durante el periodo de transición y, a partir de entonces, de forma periódica

Para obtener más información sobre el RGPD para el operador de VMS, consulte la Milestone Guía de privacidad del RGPD para operadores de VMS y el Milestone aprendizaje virtual del RGPD para operadores de VMS.

Administrador del sistema VMS

Los administradores de sistemas son responsables de la creación de un entorno de sistemas que cumpla con el RGPD. Los administradores del sistema hacen entre otras cosas lo siguiente:

- Aplicar y mantener un alto grado de seguridad general. Para obtener más información sobre cómo asegurar sus instalaciones XProtect VMS ontra los ciberataques, consulte la guía para reforzar.
- Aplicar una política de contraseñas seguras
- Efectuar auditorías de seguridad
- Asegúrese de que los dispositivos registren de acuerdo con el propósito definido, por ejemplo, en caso de evento, movimiento, siempre activo, etc.
- Garantizar que el tiempo de conservación del registro y de la auditoría se establecen de acuerdo con la legislación local y el propósito definido del VMS
- Garantizar la gestión de usuarios (añadir y eliminar usuarios)
- Asegúrese de que las cámaras cumplen las leyes de privacidad y no graban zonas que no deben ser grabadas enmascarando las zonas que no deben ser grabadas
- Póngase en contacto con el delegado de protección de datos (DPD) si se sospecha de un incumplimiento del RGPD, por ejemplo, en el caso de una violación de los datos de los materiales de vídeo (consulteAnexo: Cumplimiento del RGPD en la página 27)

Operador de VMS

Los operadores de VMS deben seguir procesos e instrucciones de trabajo cuando acceden a los datos del sistema, por ejemplo, cuando visualizan vídeos o exportan vídeos, etc.

Para cumplir con el RGPD, los operadores deben tener lo siguiente:

- Comprensión general del RGPD y de las normas de exportación de datos
- Formación sobre el RGPD

  Los operadores deben tener una formación adecuada del sistema de videovigilancia para garantizar que no se invade la intimidad y otros derechos fundamentales de los titulares de los datos captados por las cámaras. Se les debe enseñar lo que definen las políticas de videovigilancia (por ejemplo, los procedimientos de entrega de pruebas de vídeo), a quién dirigirse en caso de duda (personas de punto de referencia, como el supervisor o el responsable de la protección de datos), etc. (consulte Responsable de seguridad (supervisor del VMS) en la página 16).

  Para obtener más información sobre el RGPD para el operador de VMS, consulte la Milestone Guía de privacidad del RGPD para operadores de VMS y el Milestone aprendizaje virtual del RGPD para operadores de VMS.

Gestión de datos exportados

La exportación se realiza cuando ha habido un incidente que requiere compartir las pruebas con las autoridades. Si tiene derechos de usuario para exportar pruebas, tiene la responsabilidad de gestionarlas. El motivo por el que es sensible es tanto por el contenido como por el hecho de que los datos salen del sistema de

vigilancia. Lo más probable es que se haya producido un incidente que puede implicar una actividad delictiva. También puede haber detalles privados sensibles en las pruebas. Cuando se exporta, suele guardarse en algún tipo de soporte extraíble (unidad USB, disco óptico, etc.).

Si esos datos acaban en manos equivocadas, se perdería la privacidad de los titulares de los datos en las pruebas.

Debe tener un proceso claro para exportar las pruebas, que incluya:

- ¿Quién puede exportar pruebas?
- ¿Dónde se guardan las pruebas hasta que se entregan a las autoridades?
- ¿Quién tiene acceso a ella?
- ¿Qué formato(s) debe(n) utilizarse?
- ¿Si se debe aplicar el cifrado (muy recomendable)?
- ¿Cuándo se destruyen las pruebas?

Los responsables del tratamiento deben adoptar medidas técnicas y organizativas para proteger los datos que salen del Milestone XProtect VMS. Estas medidas podrían ser:

- Limitar el permiso para exportar vídeos y registros de auditoría sólo al personal especial
- Considerar la posibilidad de cifrar los datos antes o después de exportarlos
- Aplicar máscaras de privacidad antes de exportar los datos de vídeo, cuando sea necesario
- Proteger físicamente los soportes extraíbles con datos personales
- Establecer políticas que garanticen que los datos personales se eliminan de los soportes según el tiempo de conservación
- Lleva un registro de los soportes extraíbles: ¿quién ha exportado qué datos a los medios? ¿A quién se ha enviado y con qué fin? ¿Se informa al destinatario de que debe destruir el soporte o devolverlo una vez cumplido el propósito? Etc.
- Utilizar las políticas de grupo de Windows para deshabilitar los puertos USB o el acceso a los medios en los ordenadores del cliente.
- Monitorizar los registros de auditoría en busca de eventos de exportación no autorizados
- Comprometer a los empleados con la política de protección de datos
- Desinfectar adecuadamente los soportes o eliminarlos físicamente si no es posible la desinfección (por ejemplo, los DVD)

Consulte el Milestone aprendizaje virtual sobre el RGPD para operadores de VMS para obtener más información sobre la gestión de las exportaciones de datos.

Tratamiento de los datos exportados en las notificaciones y el correo electrónico

Además de las exportaciones, los datos también pueden extraerse del VMS mediante archivos adjuntos a las notificaciones. Las notificaciones son correos electrónicos que se envían a una dirección de correo electrónico determinada. Al crear una notificación, el administrador puede decidir incluir un conjunto de instantáneas o un AVI de una secuencia. Debido a que las instantáneas adjuntas y las secuencias AVI en las notificaciones salen del VMS, están fuera del control del VMS para el acceso y la retención del usuario. Se recomienda no adjuntar imágenes o secuencias AVI a las notificaciones por correo electrónico. Si los archivos adjuntos son necesarios, hay que asegurarse al menos de que existen procedimientos y controles organizativos sobre quién recibe los correos electrónicos y cómo se gestionan.

Debe tener un proceso claro, que cubra:

- ¿Dónde se almacenan los datos?

  Asegúrese de que los servidores de correo electrónico de envío y recepción están bajo el control de la organización que es el controlador/procesador de datos de la videovigilancia. En particular, los destinatarios no deben ser cuentas de correo electrónico en cuentas de correo gratuitas como Gmail o Hotmail, etc.

- ¿Quién tiene acceso a ella?
- ¿Qué formato(s) debe(n) utilizarse?
- ¿Debe aplicarse el cifrado SMTP?

  Tenga en cuenta que: Utilice un servidor de correo SMTP/SMTPS. Debe cifrar la conexión entre el VMS y los servidores de correo saliente, así como entre los servidores SMTP de envío y recepción para estar cubiertos por el Sello de Privacidad Europeo. Una conexión no cifrada y no segura violaría el sello EuroPriSe y llevaría a la pérdida del cumplimiento del sello de privacidad EuroPriSe.

- ¿Cuándo se destruyen los datos?

  Milestone recomienda que el tiempo de conservación de los datos de vídeo en los buzones salientes y entrantes se alinee con el tiempo de conservación de la base de datos de medios o con el tiempo de conservación de las alarmas que pueden ser activadas por los mismos eventos que causaron la notificación.

  El tiempo de conservación en los buzones debe limitarse a un límite que sea razonable para el propósito del proceso de notificación.

  Milestone recomienda utilizar únicamente los buzones del responsable del tratamiento de los datos y configurar la eliminación automática de los correos electrónicos una vez alcanzado el tiempo de conservación definido.

  Los responsables del tratamiento / procesadores de datos deben asegurarse de que estos buzones no sean archivados automáticamente por el sistema de correo electrónico.

Violación de información personal

El RGPD define una "violación de datos personales" como "una violación de la seguridad que provoque la destrucción accidental o ilegal, la pérdida, la alteración, la divulgación no autorizada o el acceso a información personal transmitida, almacenada o tratada de otro modo".

En el caso de una violación de la seguridad, el DPD debe determinar si se debe notificar a la Autoridad de protección de datos y a los titulares de los datos implicados, de acuerdo con los artículos 33 y 34 del RGPD.

De acuerdo con el artículo 33 (1) del RGPD:

> *En caso de violación de los datos personales, el encargado del tratamiento notificará la violación de los datos personales a la autoridad de control competente de conformidad con el artículo 55 sin demora indebida y, cuando sea posible, a más tardar 72 horas después de haber tenido conocimiento de ella, a menos que sea improbable que la violación de los datos personales dé lugar a un riesgo para los derechos y libertades de las personas físicas. Cuando la notificación a la autoridad de control no se realice en un plazo de 72 horas, deberá ir acompañada de los motivos del retraso.*

Si se considera necesario, el encargado del tratamiento debe publicar la notificación de la violación de datos en un plazo de 72 horas desde que tenga conocimiento de la misma (consulte Violación de información personal en la página 22). Para ver un modelo de notificación de violación de datos, consulte la plantilla *Milestone Notificación de violación de datos*. Los titulares de los datos también deben ser notificados si la violación de los datos personales "puede suponer un alto riesgo para los derechos y libertades de las personas".

Los encargados del tratamiento que experimenten una violación de los datos personales deben notificarlo al responsable del tratamiento, pero por lo demás no tienen ninguna otra obligación de notificación o de información en virtud del RGPD.

Para obtener información sobre las demás responsabilidades del DPD, consulte Controlador de datos en la página 14.

Encargado del tratamiento

Si una organización subcontrata todas o parte de sus actividades de videovigilancia a un tercero (un procesador de datos), sigue siendo responsable del cumplimiento del RGPD como controlador de datos. Por ejemplo, guardias de seguridad que supervisan la videovigilancia en directo en la zona de recepción de una organización que trabaja para una empresa privada a la que la organización ha subcontratado la tarea de monitorización en directo. En este caso, la organización debe garantizar que los guardias de seguridad realicen sus actividades de conformidad con el RGPD.

Para cumplir con el RGPD, los procesadores de datos de terceros (excluyendo las fuerzas de seguridad) deben:

- Cumplir los mismos requisitos que el operador (consulte Operador de VMS en la página 19)
- Firmar y cumplir un *Acuerdo de procesamiento de datos* (consulte Anexo: Acuerdo de procesamiento de datos en la página 54).

Resumen

El RGPD es una normativa que ya está influyendo en la forma en que las organizaciones administran los datos, incluidos los de vídeo.

Como mínimo, cada organización que procesa datos personales necesita una o más personas designadas responsables para asegurarse de que la organización gestiona los datos personales en línea con el GDPR y la política de la empresa (el número de horas de trabajo asignadas para esto dependerá del tamaño de la organización y la cantidad de datos personales recopilados y procesados). Además, para algunas organizaciones, el RGPD requerirá el nombramiento de un delegado de protección de datos (DPD) formal para realizar estas tareas.

También habrá cambios en el proceso administrativo. Bajo el RGPD, las organizaciones tienen que mantener el *Registro de actividades de procesamiento de datos* detallado y preciso. Para ver un modelo de registro de actividades de tratamiento, consulte la plantilla de *Milestone Registro de actividades de tratamiento* . Hay una serie de detalles que deben registrarse, incluidos, entre otros, los siguientes:

- La categoría de personas a la que se refieren los datos personales tratados (por ejemplo, clientes, empleados, visitantes de la tienda, etc.).
- Para qué propósitos se utilizan los datos personales
- Si los datos personales van a ser transferidos, a otras empresas y/o fuera de la UE
- Cuánto tiempo se almacenarán los datos personales
- Medidas adoptadas por la organización, en relación con cada actividad de tratamiento de datos por separado, para garantizar el cumplimiento del RGPD

Todo esto es relevante cuando se trata de vídeo de vigilancia almacenado, y definido en la política de videovigilancia (véase Anexo: Política de videovigilancia en la página 49).

Las organizaciones están obligadas a explicar por qué una cámara de vídeo está en un lugar determinado, qué se está filmando y el motivo. En el caso de la videovigilancia, se debe utilizar una señalización adecuada en la zona en la que se utiliza la videovigilancia y en sus alrededores para proporcionar información al respecto.

El responsable del tratamiento puede estar obligado a realizar una evaluación de impacto de la protección de datos (consulteAnexo: Evaluación del impacto de la protección de datos en la página 50) cuando se trata de instalar una cámara en un lugar público. Una evaluación de impacto debe incluir:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los propósitos del tratamiento
- Una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento en términos de propósito (Esto puede requerir asistencia externa)
- La evaluación del riesgo para los derechos y libertades de las personas
- Las medidas previstas para hacer frente a estos riesgos, incluidas las garantías y los mecanismos para asegurar la protección de los datos personales y el cumplimiento del RGPD (se deben tener en cuenta los derechos e intereses legítimos de las personas y otras personas afectadas)

Una de las características clave del RGPD es que las personas a las que se hace un seguimiento deben estar plenamente informadas de los datos que se guardan sobre ellas y de cómo se utilizan. El aviso de derecho de información informa a las personas afectadas de: el propósito de la vigilancia, quién conserva los datos que se recogen (responsable del tratamiento/encargado del tratamiento) y la política de conservación. Para ver un modelo de notificación en el lugar de los hechos, consulte la plantilla*Milestone Aviso en el lugar*.

Las organizaciones que almacenan vídeo tienen responsabilidades claras cuando se trata de almacenar datos personales y deben establecer medidas sólidas para evitar el acceso no autorizado. Esto significa que es importante establecer, por escrito, quién tendrá acceso a las cámaras y grabaciones.

Las organizaciones también deben contar con un procedimiento para cuando una persona decida ejercer su derecho de acceso a los datos personales o solicitar su supresión. Esto es para que puedan permanecer dentro de la ventana prescrita de un mes dentro de la cual deben cumplir con estas solicitudes de acuerdo con el RGPD. Al hacer una solicitud de este tipo, es razonable esperar que el solicitante proporcione información adecuada para localizar estos datos, por ejemplo, un período de tiempo aproximado y la ubicación en la que se capturó el vídeo. Es decir, el sujeto debe proporcionar documentos de identidad oficiales que demuestren quién es, y la organización debe dejar constancia de las grabaciones que se le muestran o proporcionan al individuo. Además, hay que enmascarar a otras personas en el vídeo, utilizando herramientas de terceros.

Las organizaciones deben utilizar medidas estrictas para evitar el acceso no autorizado a los datos personales que almacenan. Las tácticas utilizadas por cada organización serán únicas para los desafíos a los que se enfrentan. Sin embargo, en todos los casos, las organizaciones deben utilizar controles de seguridad robustos, mantenerse al día con las mejores prácticas de ciberseguridad y asegurarse de que están trabajando con socios de confianza que proporcionan hardware y software seguros, así como un cuidado posterior exhaustivo.

Tratamiento de la información personal

Al tratar la información personal, se deben respetar estos principios:

- Evaluar: Saber qué información personal tiene en sus archivos y en sus ordenadores.
- Reducir: Conservar sólo lo que necesita para su negocio.
- Proteger: Proteger la información que conserva.
- Eliminar: Deshacerse adecuadamente de lo que ya no necesita.
- Responder: Informar inmediatamente de todas las infracciones de seguridad reales o presuntas.

Para obtener más información

- Para la versión completa del *Reglamento General de Protección de Datos*
- Para obtener más información sobre el RGPD para el operador de VMS, consulte la Milestone Guía de privacidad del RGPD para operadores de VMS y el Milestone aprendizaje virtual del RGPD para operadores de VMS.
- Para estar al día y saber más sobre la evolución del RGPD, visite el sitio web de la Comisión Europea sobre Protección de Datos

- Para obtener una guía sobre el RGPD que ayude a las organizaciones a cumplir con sus requisitos, consulte la guía de la Oficina del Comisionado de Información sobre el Reglamento General de Protección de Datos del Reino Unido
- Para obtener una lista de datos clave sobre el RGPD, consulte los *datos clave sobre el Reglamento General de Protección de Datos*
- Para las recomendaciones para las instituciones y organismos europeos sobre el diseño y funcionamiento de los sistemas de videovigilancia, consulte las *directrices del Supervisor Europeo de Protección de Datos (EDPS)*
- Para obtener más información sobre cómo asegurar sus instalaciones XProtect VMS ontra los ciberataques, consulte la guía para reforzar.
- Para obtener información sobre cómo los componentes del Milestone XProtect VMS, consulte el documento Milestone que describe la arquitectura del sistema.

Milestone Plantillas del RGPD

- Plantilla *Milestone Aviso en el lugar*.
- Plantilla de *Milestone Registro de actividades de procesamiento*.
- Plantilla de*Milestone Política de videovigilancia*.

  Debe obedecer los requisitos del RGPD al establecer y desarrollar la política de videovigilancia. Tenga en cuenta que la recogida de audio y metadatos no está sujeta al Sello Europeo de Privacidad (EuroPriSe).

- *PlantillaMilestoneAcuerdo de procesamiento de datos*
- Plantilla *Milestone Solicitud del sujeto de los datos*.

  Tenga en cuenta que esto es sólo un ejemplo. No hay requisitos formales para las solicitudes de los titulares de datos.

- Plantilla *Milestone Notificación de violación de datos*.

Anexos

Para obtener información adicional, consulte las siguientes secciones:

Anexo: Cumplimiento del RGPD **27**
¿Tiene una base legal para recopilar datos? 27
Derechos individuales 33
Privacidad por diseño 38
Responsabilidad 46
Lista de comprobación para asegurar la integridad y la confidencialidad 47
Anexo: Aviso en el lugar **48**
Anexo: Política de videovigilancia **49**
Anexo: Evaluación del impacto de la protección de datos **50**
Riesgos inherentes al uso del VMS 52
Anexo: Acuerdo de procesamiento de datos **54**
Anexo: El sistema Milestone XProtect VMS y el RGPD **54**
Garantías adicionales 58
Anexo: Procesamiento de datos en el entorno de Milestone XProtect VMS **63**

Anexo: Cumplimiento del RGPD

Esta sección proporciona una visión general de la normativa del RGPD relevante para la videovigilancia. En las siguientes secciones se describe qué es el RGPD y cómo afecta al uso de la videovigilancia:

- ¿Tiene una base legal para recopilar datos? en la página 27
- Derechos individuales en la página 33
- Privacidad por diseño en la página 38
- Responsabilidad en la página 46
- Lista de comprobación para asegurar la integridad y la confidencialidad en la página 47

¿Tiene una base legal para recopilar datos?

El RGPD exige que todas las organizaciones tengan una base legal válida para recopilar y procesar datos personales.

La videovigilancia basada en el consentimiento o en los intereses vitales puede ser posible en situaciones excepcionales, por ejemplo en el sector sanitario y asistencial si hay que vigilar a una persona de forma permanente.

Usted tiene la obligación de llevar a cabo un seguimiento de las actividades de procesamiento en un *Registro de actividades de procesamiento* (artículo 30, RGPD). Para ver un modelo de registro de actividades de tratamiento, consulte la plantilla de *Milestone Registro de actividades de tratamiento* .

Compruebe la legitimidad del procesamiento de los datos de vídeo y de los datos de los usuarios de acuerdo con los siguientes niveles de regulación:

1. Reglamento general de protección de datos (artículo 6, RGPD)

   En particular, el artículo 6 (1) (b) del RGPD:

   > *El procesamiento es necesario para la ejecución de un **contrato** en el que la persona interesada es parte o puede adoptar medidas a petición de la persona interesada antes de formalizar un contrato.*

   Y el artículo 6 (1)(e)(f) del RGPD:

   > *El procesamiento será lícito si y en la medida en que sea necesario para los fines de los intereses legítimos perseguidos por el responsable del procesamiento o por un tercero, excepto cuando sobre dichos intereses prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, **en particular cuando el interesado sea un niño**.*

2. Directiva (UE) 2016/680 de aplicación de la ley o la legislación nacional basada en dicha directiva

   Cumplir con la legislación nacional basada en la Directiva (UE) 2016/680 de aplicación de la ley con el fin de establecer una base legal para comprobar la legitimidad del procesamiento.

3. Legislación nacional

   Cumplir con la legislación nacional, por ejemplo, el artículo 4 de la Ley federal alemana de protección de datos (FDPA), aunque esta disposición no se aplica a la videovigilancia realizada por empresas.

Antes de implementar la videovigilancia, evalúe los beneficios potenciales y el impacto sobre el derecho a la intimidad y otros derechos fundamentales e intereses legítimos de las personas que se encuentran en la zona contemplada.

Cuando decida utilizar la videovigilancia, documente el propósito del sistema de vídeo, qué información se recopila, para qué se utilizará, por quién y durante cuánto tiempo, y proporcione pruebas de soporte adecuadas, como datos estadísticos sobre el número real de incidentes de seguridad ocurridos, así como pruebas de la eficacia pasada de las cámaras para disuadir, prevenir, investigar o procesar esos incidentes.

El alcance de la evaluación depende del tamaño del sistema propuesto y del impacto en la intimidad de las personas y otros intereses legítimos o derechos fundamentales.

Procesamiento basado en una obligación legal o una tarea pública

¿Cuándo es probable que se aplique la base jurídica de las obligaciones legales? En resumen, cuando tenga que procesar los datos personales para cumplir con la ley. El artículo 6 (3) del RGPD exige que la obligación legal debe estar establecida por la legislación de la UE o de los estados miembros.

Este hecho no implica que deba existir una obligación legal que exija específicamente la actividad de procesamiento específica. La esencia es que su propósito general debe ser cumplir con una obligación legal que tenga una base suficientemente clara en el derecho común o en la ley. A modo de ejemplo, una orden judicial puede exigirle el procesamiento de datos personales para un fin determinado, lo que también se considera una obligación legal.

Las instituciones públicas utilizan normalmente la videovigilancia para realizar una tarea pública. Tenga en cuenta que la compensación de intereses no es una base legal para las autoridades públicas en el cumplimiento de estas tareas.

La vídeovigilancia sólo es legítima en el caso de las instituciones públicas si es necesaria para el cumplimiento de la función pública. Debe realizar una evaluación de la proporcionalidad cuando realice una tarea pública (consulte Compensación de intereses/evaluación de la proporcionalidad en la página 29). El controlador de datos debe tener en cuenta los principios de minimización de los datos (por ejemplo, enmascaramiento de la privacidad), limitación del almacenamiento (tiempo de retención) y limitación de la finalidad (artículo 5 (1), RGPD).

Compensación de intereses/evaluación de la proporcionalidad

Los organismos privados suelen operar un VMS para conseguir los intereses legítimos del responsable del procesamiento de datos o de un tercero (artículo 6 (1) (f), RGPD). Por lo tanto, es necesario equilibrar los intereses para comprobar la legitimidad del procesamiento. El controlador de datos necesita identificar y valorar sus intereses frente a los intereses o derechos y libertades fundamentales de los interesados, que requieren la protección de los datos personales.

El procesamiento de los datos de auditoría y del historial de alarmas puede basarse normalmente en el interés legítimo del responsable del tratamiento (artículo 6, apartado 1, letra f), del RGPD). Lo mismo ocurre con los datos de gestión de usuarios (datos de la cuenta, credenciales de autenticación, datos de autorización, datos de configuración) si el usuario es un empleado de una empresa de seguridad.

Debe mostrar claridad, franqueza y honestidad con la gente desde el principio sobre el uso de sus datos personales. En su evaluación, deberá abordar las siguientes cuestiones:

- ¿Cuáles son las ventajas de utilizar la videovigilancia? ¿Las ventajas superan los posibles efectos perjudiciales?
- ¿Está el propósito del sistema claramente especificado, es explícito y legítimo? ¿Existe una base legal para la videovigilancia?
- ¿La necesidad de utilizar la videovigilancia está claramente demostrada? ¿Es una herramienta eficaz para lograr su propósito? ¿Existen alternativas menos intrusivas?

Además, el controlador de datos sólo puede utilizar los datos personales para un nuevo propósito si es compatible con el propósito original, o si el controlador de datos obtiene el consentimiento o tiene una base clara por ley.

Intereses típicos del controlador de datos

Normalmente, el controlador de datos:

- Ejerce el derecho a establecer a quién se le permite o deniega el acceso a los datos
- Protege los intereses legítimos para propósitos específicamente definidos

En el contexto del empleo, el controlador de datos debe ser informado de que el procesamiento de los datos personales de los empleados, tanto de los datos de vídeo como de los datos de los usuarios, en el contexto del empleo puede estar sujeto a normas más específicas en virtud de la legislación de los estados miembros (artículo 88, RGPD), por ejemplo, la sección 26 FDPA (Alemania).

Intereses y derechos típicos de los interesados

Los interesados tienen derecho a:

- No tener una vigilancia de larga duración
- No vigilar las situaciones íntimas
- Tiempos de retención cortos
- Garantías adecuadas si se tratan categorías especiales de datos personales (artículo 9 del RGPD)

Cómo reduce XProtect el impacto sobre los intereses o los derechos y libertades fundamentales del interesado

Milestone XProtect reduce el impacto sobre los intereses y derechos fundamentales del interesado:

- Protección de datos personales a través de:
    - Control de acceso basado en funciones
        - Máscaras de privacidad únicamente elevables por el supervisor
        - Protocolo de acceso
    - Criptografiado de registros
    - Retención automática de vídeos (borrado automático)
    - Máscara de privacidad
    - Exportación de vídeo segura y verificable

- Ciberseguridad
  - Refuerzo del sistema. Para obtener más información sobre cómo asegurar sus instalaciones XProtect VMS ontra los ciberataques, consulte la guía para reforzar.
  - Notificación y aplicación de parches de vulnerabilidades conocidas. Para obtener más información, consulte Notificación y aplicación de parches de vulnerabilidades conocidas.
- Educación y concienciación
  - Programas de certificación de educación para socios
  - Programas de certificación de productos para socios (consulte Milestone Programa de socios tecnológicos y Milestone Marketplace)
  - Milestone Aprendizaje virtual sobre el RGPD para operadores de VMS

Transferencias y divulgaciones

Hay tres normas principales en el RGPD que regulan las transferencias, dependiendo de si se transfieren las grabaciones:

- A un destinatario dentro de la organización o en otra organización

  En este caso, el RGPD establece que las grabaciones pueden ser transferidas a otras personas dentro de la organización o en otra organización si esto es necesario para el desempeño legítimo de las tareas cubiertas por la competencia del destinatario.

- A otros dentro de la Unión Europea

  En este caso (transferencias fuera de las organizaciones pero dentro de la Unión Europea), son posibles si es necesario para el cumplimiento de una tarea realizada en interés público o sujeta al ejercicio de la autoridad pública, o si el destinatario establece de otro modo que la transferencia es necesaria y no hay razón para suponer que los intereses legítimos de aquellos cuyas imágenes se transfieren puedan verse perjudicados.

- O al exterior de la Unión Europea

  En este caso, se pueden realizar transferencias fuera de la Unión Europea: (i) si se hace únicamente para permitir que se lleven a cabo las tareas de la organización y (ii) sólo conforme a requisitos adicionales, principalmente para garantizar que los datos estarán adecuadamente protegidos en el extranjero.

En resumen

Asegúrese de no hacer nada con los datos que infrinja cualquier otra ley.

Debe utilizar los datos personales de manera justa. Esto significa que no debe procesar los datos de una manera que sea indebidamente perjudicial, inesperada o engañosa para las personas implicadas.

Sólo puede utilizar los datos personales para un nuevo propósito si es compatible con el propósito original, u obtiene el consentimiento o tiene una base clara por ley.

En algunos casos que se consideran de alto riesgo de violación de la intimidad, debe realizar una evaluación de impacto formalizada (consulte Anexo: Evaluación del impacto de la protección de datos en la página 50).

Realización de una evaluación de impacto

Antes de instalar e implementar sistemas de videovigilancia, debe realizar una *evaluación del impacto sobre la privacidad y la protección de datos*.

El objetivo de la evaluación de impacto es determinar el impacto del sistema propuesto sobre la privacidad de las personas y otros derechos fundamentales, así como identificar formas de mitigar o evitar cualquier efecto adverso.

¿Cuánto esfuerzo debe dedicarse a la evaluación de impacto? Depende de las circunstancias. Un sistema de videovigilancia con un alto riesgo de violación de la intimidad justifica una mayor inversión que un sistema de videovigilancia con un impacto limitado en la intimidad, por ejemplo, un sistema de CCTV estático convencional.

Como mínimo, de acuerdo con el artículo 35 (7) del RGPD, la evaluación debe contener al menos:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, incluyendo, en su caso, el interés legítimo perseguido por el responsable del tratamiento
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en relación con los propósitos
- Una evaluación de los riesgos para los derechos y libertades de los titulares de los datos a los que se refiere el artículo 35 (1) del RGPD:

  Donde un tipo de tratamiento, en particular que utiliza nuevas tecnologías, y teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, pueda suponer un riesgo elevado para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de los datos personales. Una única evaluación puede referirse a un conjunto de operaciones de transformación similares que presentan riesgos elevados parecidos.
- Las medidas previstas para hacer frente a los riesgos, incluidas garantías, medidas de seguridad y mecanismos para garantizar la protección de los datos personales y demostrar el cumplimiento del RGPD teniendo en cuenta los derechos e intereses legítimos de los interesados y otras personas afectadas

En cualquier caso, y en todos los casos, debe calcular y justificar si se recurre a la videovigilancia, cómo colocar las cámaras, seleccionar y configurar los sistemas, y cómo aplicar las garantías de protección de datos necesarias. Para obtener información sobre sus instalaciones XProtect VMS, consulte la guía para reforzar y la guía de certificados.

Derechos individuales

Uno de los principales propósitos del RGPD es dar a las personas una mayor protección y un conjunto de derechos que regulen sus datos personales.

Hay algunos requisitos muy específicos en las condiciones del reglamento, todas las cuales significan que la parte que procesa o almacena datos personales tiene la responsabilidad de mantener estos datos privados.

El RGPD otorga a las personas el derecho a saber cuándo se recogen sus datos personales (en el punto de captación) y cómo se van a utilizar. En el caso de la videovigilancia, por ejemplo, se trata de una señalización adecuada en la zona en la que se utiliza la videovigilancia y en sus alrededores.

Los artículos 12 a 23 del RGPD cubren los derechos del titular de datos.

- Sección 1: Transparencia y modalidades
  - Artículo 12: Información, comunicación y modalidades transparentes para el ejercicio de los derechos del titular de los datos
- Sección 2: Información y acceso para los datos personales
  - Artículo 13: Información que debe facilitarse cuando se recojan datos personales del titular de los datos
  - Artículo 14: Información que debe facilitarse cuando los datos personales no se hayan obtenido del titular de los datos
  - Artículo 15: Derecho de acceso del titular de los datos (consulte Derecho de acceso en la página 34)
- Sección 3: Rectificación y eliminación
  - Artículo 16: Derecho de rectificación
  - Artículo 17: Derecho al olvido (Derecho a la supresión) (consulte Derecho al olvido (Derecho a la supresión) en la página 36)
  - Artículo 18: Derecho a la limitación del tratamiento (consulteDerecho a la limitación del tratamiento en la página 38)
  - Artículo 19: Obligación de notificar la rectificación o supresión de los datos personales o la limitación del tratamiento
  - Artículo 20: Derecho a la portabilidad de los datos
- Sección 4: Derecho de oposición y toma de decisión individual automatizada
  - Artículo 21: Derecho de oposición
  - Artículo 22: Toma de decisión individual automatizada, incluida la elaboración de perfiles
- Sección 5: Restricciones
  - Artículo 23: Restricciones

De ellos, los derechos más relevantes en el contexto de la videovigilancia son:

El derecho a la información (artículos 12 a 14 y 34, RGPD)	El artículo 12 trata de la transparencia y las modalidades, mientras que los artículos 13 y 14 tratan sobre la información y el acceso a los datos personales. Estos artículos ofrecen al titular de los datos la posibilidad de recibir información sobre qué datos personales se recogen y durante cuánto tiempo se conservan. En el contexto del VMS, consulte Anexo: Aviso en el lugar en la página 48. El artículo 34 proporciona al titular de los datos el derecho a recibir información en caso de que se produzca una violación de los datos si ésta puede suponer un alto riesgo para los derechos y libertades del titular.
El derecho de acceso (Artículo 15, RGPD)	Este derecho proporciona al titular de los datos la posibilidad de acceder a sus datos personales que están siendo procesados, por ejemplo, grabaciones de vídeo del titular. El titular de los datos tiene derecho a solicitar a una empresa información sobre qué datos personales (sobre él o ella) se están procesando y la justificación de dicho tratamiento.
El derecho a la supresión ("derecho al olvido") (Artículo 17, RGPD)	Este derecho proporciona al titular de los datos la posibilidad de solicitar la supresión de sus datos. En el contexto del VMS, la supresión a petición de los interesados es excepcional debido a los intereses del responsable del tratamiento y a los breves plazos de conservación. (Consulte Anexo: Política de videovigilancia en la página 49 y *Eliminar parcialmente grabaciones de vídeo* en Anexo: El sistema Milestone XProtect VMS y el RGPD en la página 54).
El derecho de oposición (Artículo 21, RGPD)	Este derecho proporciona al titular de los datos la posibilidad de oponerse al tratamiento de sus datos personales. En el contexto del VMS, otros intereses, como los intereses legítimos (detección de fraudes, salud y seguridad), las obligaciones legales (contabilidad, lavado de dinero) o incluso el cumplimiento contractual (contratos de trabajo), pueden prevalecer sobre los intereses y derechos del titular de los datos. En todos los casos, esto debe ser totalmente transparente para que el titular de los datos pueda conocerlo y oponerse. Si el titular de los datos se opone, el responsable del tratamiento debe valorar la objeción o, de lo contrario, podría enfrentarse a una multa.

Para el cumplimiento del RGPD en los sistemas VMS, hay tres derechos especialmente relevantes: el derecho a ser informado, el derecho de acceso y el derecho al olvido.

Derecho de acceso

En virtud del artículo 15, el RGPD proporciona a las personas el control de sus datos personales, incluido el derecho a verlos. Es de especial importancia el derecho a que los titulares de los datos puedan obtener una copia de los mismos y a que se enmascare a terceras personas (utilizando herramientas de terceros).

A demanda del interesado, las organizaciones deben entregarle todos los datos personales recogidos sobre él, incluido el vídeo recogido por un sistema de videovigilancia.

Asegúrese de establecer procedimientos y políticas formales para gestionar las solicitudes de derecho de acceso, descritas en el *Registro de transferencias y divulgaciones*.

Transferencias y divulgaciones

Hay tres normas principales en el RGPD que regulan las transferencias, dependiendo de si se transfieren las grabaciones:

- A un destinatario dentro de la organización o en otra organización

  En este caso, el RGPD establece que las grabaciones pueden ser transferidas a otras personas dentro de la organización o en otra organización si esto es necesario para el desempeño legítimo de las tareas cubiertas por la competencia del destinatario.

- A otros dentro de la Unión Europea

  En este caso (transferencias fuera de las organizaciones pero dentro de la Unión Europea), son posibles si es necesario para el cumplimiento de una tarea realizada en interés público o sujeta al ejercicio de la autoridad pública, o si el destinatario establece de otro modo que la transferencia es necesaria y no hay razón para suponer que los intereses legítimos de aquellos cuyas imágenes se transfieren puedan verse perjudicados.

- O al exterior de la Unión Europea

  En este caso, se pueden realizar transferencias fuera de la Unión Europea: (i) si se hace únicamente para permitir que se lleven a cabo las tareas de la organización y (ii) sólo conforme a requisitos adicionales, principalmente para garantizar que los datos estarán adecuadamente protegidos en el extranjero.

Registro de transferencias y divulgaciones

Las organizaciones deben llevar un registro, siempre que sea posible, en formato electrónico, de las transferencias y divulgaciones. En él, se debe registrar cada transferencia a un tercero. (los terceros también incluyen a cualquier persona dentro de la organización a la que los que tienen acceso a las grabaciones le hagan una transferencia en primer lugar. Esto incluye normalmente cualquier transferencia fuera de la unidad de seguridad). El registro, además, debe contener todas las instancias en las que, aunque no se haya transferido la copia de la grabación de videovigilancia, se hayan mostrado las grabaciones a terceros o cuando el contenido de las grabaciones se haya divulgado de otro modo a terceros.

El registro debe incluir al menos lo siguiente:

- Fecha de los registros
- Parte demandante (nombre, título y organización)
- Nombre y título de la persona que autoriza la transferencia

- Breve descripción del contenido de las grabaciones
- Motivo de la solicitud y la razón para concederla
- Si se transfirió una copia de la grabación, se mostró la grabación o se dio información verbal

Derecho al olvido (Derecho a la supresión)

En virtud del artículo 17, el RGPD proporiciona a las personas el control sobre sus datos personales, incluido el derecho a que se borren sus datos personales si ya no son necesarios para los fines previstos del sistema.

Según el artículo 17 (1) (c) del RGPD, el responsable del tratamiento debe gestionar las objeciones de los titulares de datos. Ya que no es práctico borrar un tema específico del vídeo, los procesadores de datos deben limitar estrictamente el tiempo de retención del vídeo de acuerdo con el propósito documentado del sistema.

¿Qué debe hacer?

Revisar el tiempo de retención de todas las cámaras y asegurarse de que se establece de acuerdo con el propósito documentado del sistema.

El derecho al olvido no suele aplicarse a la videovigilancia, ya que el tiempo de retención suele ser breve y porque hay otros fundamentos jurídicos que prevalecen sobre los intereses técnicos y legales "razonables", como la obligación legal (ley de empleo), el interés público (prevención de la delincuencia, salud y seguridad públicas), los intereses vitales (datos críticos para la vida y la salud, entornos peligrosos), los intereses legítimos (detección de fraudes, empleo, desarrollo de productos), o incluso el cumplimiento contractual (empleo, suscripciones y licencias). Un ejemplo de interés legítimo es que las grabaciones de videovigilancia deben ser una fuente fiable de pruebas en cualquier momento, por lo que el VMS protege principalmente las pruebas de vídeo para que no sean manipuladas y asegura su autentificación, haciendo que el derecho al olvido sea secundario.

Normalmente hay dos razones para que los titulares de los datos se opongan al almacenamiento de las grabaciones de vídeo:

- Los intereses del responsable del tratamiento para almacenar los datos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado que exigen la protección de los datos personales (artículo 17, apartado 1, letra c), del RGPD)
- Los datos personales han sido tratados ilegalmente, por ejemplo, la vigilancia de una guardería o de un vestuario (artículo 17 (1) (d), RGPD)

Por lo tanto, cada solicitud debe ser examinada a fondo.

¿Cuánto tiempo deberían conservarse las grabaciones?

El principio general es que las grabaciones no deben ser conservadas más tiempo del necesario para los fines específicos para los que fueron realizadas. También hay que considerar si la grabación es necesaria en primer lugar y si la supervisión en directo sin grabación sería suficiente.

Si una organización escoge la grabación, debe especificar el periodo en que se conservarán las grabaciones. Después de este periodo, las grabaciones deben ser borradas. Milestone XProtect VMS automatiza el proceso de supresión, borrando automáticamente las grabaciones más antiguas que el tiempo de retención establecido.

Cuando los archivos que contienen los datos de vídeo grabados son eliminados por el VMS, los archivos y su contenido no se borran realmente de los bloques de datos del sistema de almacenamiento, sino que simplemente se marcan como libres en el sistema de archivos, lo que permite que se escriban otros archivos en esta ubicación del sistema de almacenamiento. Hasta que los bloques de datos sean realmente sobrescritos con nuevos datos, los datos de vídeo antiguos borrados pueden ser potencialmente restaurados, proporcionando acceso a grabaciones más antiguas que el tiempo de retención establecido.

Por este motivo, se recomienda no sobredimensionar el sistema de almacenamiento, ya que el riesgo aumenta con el tamaño de la sobrecarga.

Por ejemplo, si el sistema de almacenamiento asignado es el doble de grande que la cantidad de datos de vídeo almacenados para el tiempo de retención establecido, por ejemplo siete días, los bloques de datos eliminados que contienen datos de vídeo antiguos eliminados pueden permanecer estadísticamente en el sistema de almacenamiento durante siete días más antes de ser sobrescritos.

Para reducir aún más el riesgo de acceder a datos de vídeo antiguos que han sido borrados, y por seguridad en general, se recomienda habilitar el cifrado de las bases de datos multimedia, ya que esto, además de restaurar los archivos borrados, ahora también requiere romper el cifrado.

Más allá de que los datos de video hayan sido cifrados o no, una vez que los discos del sistema de almacenamiento ya no son utilizables, es importante que desinfecte o destruya físicamente los discos duros que han sido utilizados para almacenar bases de datos multimedia antes de deshacerse de ellos (por ejemplo, mediante la trituración u otro medio equivalente).

Para obtener información sobre cómo configurar esto en Milestone XProtect, consulte la sección Almacenamiento y archivo (explicación) en el manual del administrador para VMS XProtect.

Si el propósito de la videovigilancia es la seguridad, y se produce un incidente de seguridad y se determina que las grabaciones son necesarias para seguir investigando el incidente o utilizar las grabaciones como prueba, la grabación correspondiente podrá conservarse más allá de los períodos normales de retención durante el tiempo que sea necesario para estos fines. No obstante, a partir de ahí, también deben ser borrados.

Período de conservación para fines típicos de seguridad: de una semana a un mes

Cuando se instalan cámaras con propósitos de seguridad, entre una semana y un mes debería ser tiempo suficiente para que el personal de seguridad tome una decisión informada sobre la conveniencia de conservar una grabación durante un periodo más largo para seguir investigando un incidente de seguridad o utilizarla como prueba.

Un ejemplo de legislación local: según algunas autoridades alemanas de protección de datos y la mayor parte de la bibliografía sobre protección de datos, este periodo de conservación es de 48 a 72 horas como orientación para el control de acceso y la investigación de delitos penales.

Estado miembro o territorio de un tercer país: 48 horas

En caso de que la vigilancia cubra alguna zona fuera de los edificios en el territorio de un estado miembro (o de un tercer país) (normalmente las que están cerca de las zonas de entrada y salida) y no sea posible evitar que los transeúntes o los coches que pasan sean captados por las cámaras, se recomienda reducir el periodo de conservación a 48 horas o tener en cuenta de otro modo las preocupaciones locales siempre que sea posible.

Derecho a la limitación del tratamiento

El titular de los datos puede, con referencia al artículo 18 (1) del RGPD, reclamar el derecho a la restricción del tratamiento. En un escenario básico de VMS, el titular de los datos puede alegar que el tratamiento de VMS es ilegal, por ejemplo, si el titular de los datos no es consciente de que la videovigilancia de un espacio público se realiza con protección de la máscara de privacidad. Se recomienda utilizar una plantilla de *solicitud del titular de los datos* para documentar la reclamación (consulte Solicitud del titular de los datos en la página 11). Para ver un modelo de solicitud del titular de los datos, consulte la plantilla *Milestone Solicitud del titular de los datos*.

La petición debe tramitarse en un plazo razonable, más rápido que el periodo de conservación, para evitar la retención o el borrado automático de las pruebas del VMS en la petición. Por lo general, se aconseja solicitar asesoramiento legal en relación con la limitación del tratamiento. Una forma de manejar dicha solicitud es permitir que el administrador del VMS limite a los supervisores u operadores del VMS por asignación de funciones para que sólo puedan reproducir las grabaciones dentro de un corto período de tiempo después de haber sido grabadas, por ejemplo, cuatro horas o un día (consulte ¿Qué debe hacer? en la página 39: "Considere la posibilidad de restringir el acceso de los operadores a los vídeos grabados, ya sea por completo, sólo a los vídeos grabados en las últimas horas, o sólo con doble autorización"). Las limitaciones de la reproducción también se aplican a los bloqueos de pruebas. Si es necesario restringir aún más el tratamiento, se recomienda realizar tanto una evaluación del impacto sobre la empresa como una evaluación del impacto sobre la privacidad (consulte Realización de una evaluación de impacto en la página 32) como parte de la atención de las reclamaciones.

Privacidad por diseño

El RGPD exige que la privacidad debe ser una prioridad en todo el diseño del sistema y la puesta en marcha. El enfoque adoptado con respecto a la privacidad de los datos debe ser proactivo, no reactivo. Los riesgos deben anticiparse y el objetivo debe ser prevenir los acontecimientos antes de que se produzcan.

Las organizaciones deben analizar y documentar cuidadosamente cómo se diseñan los sistemas para mantenerse dentro de los objetivos establecidos.

Se debe tener cuidado de no captar datos personales de sujetos que queden fuera del dominio del sistema (por ejemplo, zonas públicas adyacentes).

Consideración detallada de quién necesita ver qué información (por ejemplo, en directo/grabada, marco temporal, resolución) y quién puede acceder a qué funciones (por ejemplo, búsqueda).

¿Qué debe hacer?

- Documentar la resolución de diferentes puntos en la escena de la cámara
- Documentar el tiempo de conservación previsto
- Considerar la posibilidad de aplicar una máscara de privacidad, permanente o elevable
- Considerar la posibilidad de establecer permisos para ver vídeos en directo, grabaciones
- Considerar la posibilidad de limitar el acceso para exportar las grabaciones y para retirar las máscaras de privacidad
- Revisar periódicamente las funciones y responsabilidades de los operadores, investigadores, administradores del sistema y otras personas con acceso al sistema
- Considerar la posibilidad de limitar el acceso a los grupos encargados de las investigaciones de las cámaras que se colocan específicamente para captar la identidad (por ejemplo, las caras de las personas que entran en una tienda)
- Considere la posibilidad de restringir el acceso de los operadores a los vídeos grabados, ya sea por completo, sólo a los vídeos grabados en las últimas horas, o sólo con doble autorización
- Limitar el número de usuarios que tienen un rol de administrador

Requisitos para la privacidad por diseño

Minimización de datos	Debe asegurarse de que los datos personales que está tratando sean: • adecuados: suficientes para cumplir correctamente con su propósito declarado • relevantes: tengan un vínculo racional con ese propósito • limitados a lo que es necesario: no tener más de lo que se necesita para ese fin.
Precisión	En general, para los datos personales: • Debe tomar todas las medidas razonables para asegurarse de que los datos personales que tiene no son incorrectos o engañosos en cuanto a cualquier hecho. • Es posible que necesite mantener los datos personales actualizados, aunque esto dependerá de para qué los utilice.

	• Si descubre que los datos personales son incorrectos o confusos, debe tomar medidas razonables para corregirlos o borrarlos lo antes posible. • Debe analizar cuidadosamente cualquier desafío a la exactitud de los datos personales.
Limitación del periodo de almacenamiento	• No debe conservar los datos personales durante más tiempo del necesario. • Hay que pensar, y poder justificar, cuánto tiempo se conservan los datos personales. Esto dependerá de sus propósitos para conservar los datos. • Necesita una política que establezca períodos de conservación estándar siempre que sea posible, para cumplir con los requisitos documentados. • También debe revisar periódicamente los datos que tiene, y borrarlos o anonimizarlos cuando ya no los necesite. • Debe considerar cuidadosamente cualquier desafío a su retención de datos. Las personas tienen derecho de supresión si usted ya no necesita los datos. • Puede conservar los datos personales durante más tiempo si sólo los mantiene para el archivo de interés público, la investigación científica o histórica, o con fines estadísticos.

Privacidad por diseño y privacidad por defecto

Según el RGPD, el responsable del tratamiento de datos personales, al tratar dichos datos, debe aplicar medidas técnicas u organizativas diseñadas para aplicar los principios de protección de datos establecidos en el RGPD. El RGPD se refiere a esto como privacidad por diseño.

En el contexto de una cámara, un ejemplo relevante de privacidad por diseño sería una característica que permite digitalmente al usuario restringir la captura de imágenes a un determinado perímetro, impidiendo que la cámara capture cualquier imagen fuera de este perímetro que de otro modo sería capturada.

En el VMS XProtect, hay soporte para el enmascaramiento de privacidad en dos formas: máscaras permanentes que no pueden ser retiradas, y máscaras que pueden ser retiradas (con los permisos adecuados) para revelar la imagen detrás de la máscara.

El responsable del tratamiento también debe aplicar medidas técnicas u organizativas que, por defecto, garanticen el tratamiento menos intrusivo para la privacidad de los datos personales en cuestión. El RGPD se refiere a esto como privacidad por defecto. En el contexto de una cámara, un ejemplo de privacidad apropiado por defecto podría ser el uso de la máscara de privacidad para mantener privada un área que sea sensible dentro de la vista de la cámara.

¿Cuál es un ejemplo de una característica de XProtect que soporta el enfoque de privacidad por diseño?

Milestone desarrolla continuamente su cartera de productos, y la privacidad por defecto es un criterio de evaluación clave para hacer que XProtect cumpla con el RGPD. Para obtener más información, consulte la guía sobre el ciclo de vida del desarrollo seguro en Milestone. Esta guía es una parte esencial de la privacidad por defecto, con la aplicación de principios como el de "defensa en profundidad", el de "mínimos privilegios" y el de evitar las configuraciones por defecto menos seguras y desactivar las funciones de uso poco frecuente por defecto.

¿Qué hay que hacer para garantizar la privacidad por diseño?

- Considerar la resolución de los diferentes puntos de la escena de la cámara y documentar estos ajustes

  Diferentes propósitos requieren diferentes calidades de imagen. Cuando la identificación no es necesaria, la resolución de la cámara y otros factores modificables deben ser elegidos para garantizar que no se capturen imágenes faciales reconocibles.

- Cifrar sus grabaciones

  Milestone recomienda que proteja sus grabaciones activando al menos un cifrado ligero en el almacenamiento y los archivos de sus servidores de grabación. Milestone utiliza el algoritmo AES-256 para el cifrado. Cuando selecciona el cifrado ligero, sólo se cifra una parte de la grabación. Cuando se selecciona cifrado fuerte, se cifra toda la grabación.

- Asegurar la red

  Milestone recomienda que seleccione cámaras que soporten HTTPS. Se recomienda configurar las cámaras en VLAN separadas y utilizar HTTPS para la comunicación entre la cámara y el servidor de grabación, así como para la comunicación entre los clientes y el servidor de grabación.

  Se recomienda activar el cifrado de la comunicación de los medios de comunicación del Recording Server a otros servidores y clientes.

  Se recomienda que XProtect Smart Client y XProtect Smart Wall están en la misma VLAN que los servidores.

  Utilice una red cifrada VPN o similar si utiliza Smart Client o Smart Wall desde una ubicación a distancia.

- Habilitar y documentar el tiempo de conservación previsto

  Según el artículo 17 (1)(a) del RGPD, las grabaciones no deben conservarse más tiempo del necesario para los propósitos específicos para los que se realizaron. Milestone recomienda establecer el tiempo de conservación de forma adecuada. De este modo, se automatiza la eliminación del vídeo.

- Exportaciones seguras

  Milestone recomienda que sólo permita el acceso a la funcionalidad de exportación a un conjunto selecto de usuarios que necesitan este permiso.

  Milestone también recomienda que el perfil Smart Client se cambie para permitir sólo la exportación en formato XProtect con el cifrado activado. Las exportaciones de AVI y JPEG no deberían estar permitidas, porque no se pueden hacer seguras. Esto hace que la exportación de cualquier material explicativo esté protegido por contraseña, cifrado y firmado digitalmente, lo que garantiza que el material forense es auténtico, no está manipulado y sólo lo ve el receptor autorizado.

- Activar máscara de privacidad, permanente o elevable

  Utilice la máscara de privacidad para ayudar a eliminar la vigilancia de áreas irrelevantes para su objetivo de vigilancia.

- Restringir los derechos de acceso con roles

  Aplicar el principio del mínimo privilegio (PoLP).

  Milestone recomienda que sólo permita el acceso a la funcionalidad a un conjunto selecto de usuarios que necesitan este permiso. Por defecto, sólo el administrador del sistema puede acceder al mismo y realizar tareas. Todos los nuevos roles y usuarios que se crean no tienen acceso a ninguna función hasta que son configurados deliberadamente por un administrador.

  Configure los permisos para todas las funciones, incluida la visualización de vídeo en directo y las grabaciones, la escucha de audio, el acceso a los metadatos, el control de las cámaras PTZ, el acceso y la configuración de Smart Wall, la retirada de las máscaras de privacidad, el trabajo con las exportaciones, el almacenamiento de instantáneas, etc.

  Restrinja el acceso a los vídeos, audios y metadatos grabados para los operadores, ya sea por completo, o restrinja el acceso sólo a los vídeos, audios o metadatos grabados en las últimas horas o menos.

  Evaluar y revisar periódicamente las funciones y responsabilidades de los operadores, investigadores, administradores del sistema y otras personas con acceso al sistema. ¿Se sigue aplicando el principio del mínimo privilegio?

- Limitar los permisos de administrador

  Milestone recomienda que limite el número de usuarios que tienen un rol de administrador.

Instalación y configuración del sistema de videovigilancia

El principio rector en lo que respecta a todos los puntos abordados en esta sección debe ser minimizar cualquier impacto negativo sobre la privacidad y otros derechos fundamentales e intereses legítimos de las personas vigiladas.

Ubicación de las cámaras y ángulos de visión

Se debe elegir la ubicación de las cámaras para minimizar las zonas de visión que no sean relevantes para los propósitos previstos.

Por regla general, allí donde se instale un sistema de videovigilancia para proteger los activos (bienes o información) de la organización o la seguridad del personal y los visitantes, la organización debe limitar la monitorización a

- áreas cuidadosamente seleccionadas que contienen información sensible, artículos de alto valor u otros activos que requieran una mayor protección por una razón concreta,
- los puntos de entrada y salida de los edificios (incluidas salidas de emergencia y salidas de incendios y muros o vallas que rodean el edificio o la propiedad), y
- los puntos de entrada y salida dentro del edificio que conectan distintas zonas sujetas a diferentes derechos de acceso y separadas por puertas cerradas u otro mecanismo de control de acceso.

Número de cámaras

El número de cámaras a instalar dependerá del tamaño de los edificios y de las necesidades de seguridad que, a su vez, dependen de diferentes factores. El mismo número y tipo de cámaras puede ser adecuado para una organización y puede ser enormemente desproporcionado para otra. No obstante, en igualdad de condiciones, el número de cámaras es un buen indicador de la complejidad y el tamaño de un sistema de vigilancia y puede sugerir mayores riesgos para la privacidad y otros derechos fundamentales. Conforme aumenta el número de cámaras, también aumenta la probabilidad de que no se utilicen de forma eficiente y se produzca un exceso de información. Por ello, el Supervisor Europeo de Protección de Datos (SEPD) recomienda limitar el número de cámaras a lo estrictamente necesario para lograr los propósitos del sistema. El número de cámaras debe figurar en la política de videovigilancia.

Horas de monitorización

La hora a la que se configuran las cámaras están programadas para grabar para minimizar la vigilancia en horas que no son relevantes para los propósitos previstos. Si el propósito de la videovigilancia es la seguridad, siempre que sea posible, el sistema debe configurarse para que grabe sólo durante las horas en las que hay una mayor probabilidad de que se produzcan los supuestos problemas de seguridad.

Resolución y calidad de imagen

Se debe elegir una resolución y una calidad de imagen adecuadas. Diferentes propósitos requerirán diferentes calidades de imagen. Por ejemplo, cuando la identificación de los individuos es esencial, la resolución de las cámaras, los ajustes de compresión en un sistema digital, la ubicación, la iluminación y otros factores deben ser tenidos en cuenta y elegidos o modificados para que la calidad de la imagen resultante sea suficiente para proporcionar imágenes faciales reconocibles. Si la identificación no es necesaria, la resolución de la cámara y otros factores modificables pueden ser elegidos para garantizar que no se capturen imágenes faciales reconocibles.

¿Quién debe tener acceso al VMS?

Sólo un número reducido de personas, claramente identificadas, podrá acceder a los datos en función de una necesidad estricta de acceso. Las políticas de acceso al VMS deben ser definidas siguiendo el principio de "mínimo privilegio": el derecho de acceso a los usuarios debe ser concedido sólo a aquellos recursos que sean estrictamente necesarios para llevar a cabo sus tareas.

Sólo el responsable del tratamiento, el administrador del sistema u otros miembros del personal designados específicamente por el responsable del tratamiento para este propósito deben poder conceder, modificar o anular los derechos de acceso de cualquier persona. Cualquier provisión, alteración o anulación de los derechos de acceso debe hacerse de acuerdo con los criterios establecidos en la política de videovigilancia de la organización.

Las personas que tengan permiso de acceso deben ser siempre personas claramente identificables.

La política de videovigilancia debe especificar y documentar claramente quién tiene acceso a las grabaciones de videovigilancia y/o a la arquitectura técnica, por ejemplo los servidores VMS, del sistema de videovigilancia, con qué propósito y en qué consisten esos derechos de acceso. En particular, debe especificar quién tiene derecho a

- Ver el vídeo/audio en tiempo real
- Operar las cámaras panorámicas, inclinadas y con zoom (PTZ)
- Ver las grabaciones
- Exportar, o
- Eliminar cualquier grabación

Además, debe configurar el acceso para las siguientes funciones del VMS:

- Marcadores
- Bloqueos de evidencias
- Retirar máscaras de privacidad
- Exportar
- Eventos iniciadores
- Iniciar/detener grabación
- Crear/editar/borrar/activar/bloquear/retirar valores preestablecidos de PTZ
- Crear/editar/borrar/iniciar/detener esquemas de patrulla PTZ
- Búsqueda avanzada
- Permisos de audio, metadatos, E/S y eventos

Protección de los datos almacenados y transmitidos

En primer lugar, se debe realizar un análisis interno de los riesgos de seguridad para determinar qué medidas de seguridad son necesarias para proteger el sistema de videovigilancia, incluidos los datos personales tratados.

En todos los casos, deben tomarse medidas para garantizar la seguridad en relación con

- Transmisión
- Almacenamiento (como en bases de datos informáticas)
- Acceso (como el acceso a servidores, sistemas de almacenamiento, la red y las instalaciones)

La transmisión debe canalizarse a través de canales de comunicación seguros y estar protegida contra la interceptación, por ejemplo, mediante:

- Cifrado de los medios de Recording Server a los servidores y clientes
- Cámara HTTPS al Recording Server
- VPN para Smart Client o Management Client conectado a través de Internet

La protección contra la interceptación es especialmente importante si se utiliza un sistema de transmisión inalámbrica o si se transfieren datos a través de Internet. En estos casos, los datos deben ser cifrados mientras están en tránsito, o se debe proporcionar una protección equivalente.

El cifrado u otros medios técnicos que garanticen una protección equivalente también deben considerarse en otros casos, mientras están almacenados, si el análisis interno de los riesgos de seguridad lo justifica. Este puede ser el caso, por ejemplo, si los datos son especialmente delicados. Mediante el cifrado de la base de datos de los medios se consigue esto.

Todas las instalaciones en las que se almacenan los datos de videovigilancia y en las que se visualizan deben ser seguras. El acceso a la sala de control y a la sala de servidores donde se encuentran los servidores VMS debe estar protegido. Ningún tercero (por ejemplo, personal de limpieza o de mantenimiento) debe tener acceso sin supervisión a estas instalaciones.

Los monitores deben colocarse de forma que el personal no autorizado no pueda observarlos. Si deben estar cerca de zonas públicas, los monitores deben colocarse de forma que sólo el personal de seguridad pueda verlos.

El XProtect VMS registra información básica por defecto, pero le recomendamos que habilite el registro de acceso de los usuarios en el Management Client para el registro de auditoría.

Este sistema de registro digital sirve para garantizar que una auditoría pueda determinar en cualquier momento quién ha accedido al sistema, dónde y cuándo. El sistema de registro puede identificar quién ha visto, borrado o exportado cualquier dato de videovigilancia (esto requiere que se habilite el registro de acceso de los usuarios).

Para obtener más información, consulte el manual de administrator para XProtect VMS.

A este efecto, y a otros, hay que prestar atención a las funciones y competencias clave de los administradores del sistema, y a la necesidad de equilibrarlas con una supervisión y unas garantías adecuadas.

Responsabilidad

El artículo 5 (2) del RGPD establece:

El responsable del tratamiento debe responsabilizarse del cumplimiento del apartado 1 ("responsabilidad") y poder demostrarlo.

Los principios relativos al tratamiento de datos personales son: legalidad, equidad y transparencia, limitación del propósito, minimización de los datos, exactitud, limitación del almacenamiento, integridad y confidencialidad.

El principio de responsabilidad requiere que asuma la responsabilidad de lo que hace con los datos personales.

Más específicamente, el artículo 30 del GDP establece:

Cada responsable del tratamiento y, en su caso, su representante, mantendrá un registro de las actividades de tratamiento bajo su responsabilidad.

El registro debe contener toda la siguiente información:

a. *el nombre y los datos de contacto del responsable del tratamiento y, en su caso, del responsable conjunto, del representante del responsable del tratamiento y del delegado de protección de datos*

b. *los propósitos del tratamiento*

c. *una descripción de las categorías de titulares de datos y de las categorías de datos personales*

d. *las categorías de destinatarios a quienes se han comunicado o se comunicarán los datos personales, incluidos los destinatarios de terceros países u organizaciones internacionales*

e. *cuando proceda, las transferencias de datos personales a un tercer país o a una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias mencionadas en el subpárrafo del artículo 49 (1), la documentación de las garantías adecuadas*

f. *cuando proceda, los plazos previstos para la supresión de las distintas categorías de datos*

g. *cuando proceda, una descripción general de las medidas de seguridad técnicas y organizativas a que se refiere el artículo 32 (1).*

La responsabilidad es uno de los principios de la protección de datos: le hace responsable de cumplir con el RGPD y dice que debe ser capaz de demostrar su cumplimiento.

Tiene que poner en marcha las medidas técnicas y organizativas adecuadas para cumplir con los requisitos de responsabilidad.

Hay varias medidas que puede tomar, y que incluso debe tomar en algunos casos, entre ellas:

- Adoptar y aplicar políticas de protección de datos
- Tomar un enfoque de "protección de datos por diseño y por defecto" (para más información, consulte Privacidad por diseño en la página 38)
- Formalizar contratos por escrito con las organizaciones que procesan datos personales en su nombre

- Mantener la documentación de sus actividades de tratamiento
- Implementar las medidas de seguridad adecuadas
- Registrar y, en caso necesario, notificar las violaciones de los datos personales
- Realizar evaluaciones de impacto de la protección de datos para los usos de los datos personales que puedan suponer un alto riesgo para los intereses de las personas
- Nombrar a un delegado de protección de datos
- Respetar los códigos de conducta pertinentes y firmar los esquemas de certificación

Utilice una plantilla de registro de actividades de procesamiento para identificar y hacer un seguimiento de los problemas de responsabilidad. Para ver un modelo de registro de actividades de tratamiento, consulte la plantilla de *Milestone Registro de actividades de tratamiento* .

Las obligaciones de responsabilidad están en curso. Las obligaciones de responsabilidad están en curso.

Si implementa un marco de gestión de privacidad, esto puede ayudarle a integrar sus medidas de responsabilidad y crear una cultura de privacidad en toda su organización.

Ser responsable puede ayudarle a crear confianza con las personas y puede ayudarle a mitigar las acciones de aplicación del RGPD.

Lista de comprobación para asegurar la integridad y la confidencialidad

El RGPD exige que las organizaciones dispongan de políticas y procedimientos exhaustivos que garanticen que los datos personales permanezcan siempre en poder de la organización. Además, las violaciones de datos personales deben comunicarse dentro de las 72 horas siguientes a la autoridad de control competente designada por el gobierno de su país.

Proteger los datos personales con todas las medidas organizativas y técnicas apropiadas.

¿Qué debe hacer?

- Revisar las políticas de seguridad en relación con el control de las contraseñas y el uso de las cuentas.
- Considerar la posibilidad de establecer requisitos mínimos de seguridad de la contraseña para todos los grupos de dominio. Considerar la posibilidad de establecer requisitos más estrictos para las cuentas administrativas a nivel de dominio.
- Contar con procesos para auditar el estado de la protección y detectar infracciones.
- Asegurarse de que los usuarios no compartan cuentas, ya sea compartiendo contraseñas o no cerrando o iniciando la sesión al final o al comienzo de su turno.
- Mantener una política y un procedimiento documentados que regulen las acciones apropiadas en el caso de una violación de datos.

- Debe garantizar que cuenta con las medidas de seguridad adecuadas para proteger los datos personales que posee.
- Un principio clave del RGPD es que procese los datos personales de forma segura mediante "medidas técnicas y organizativas apropiadas": es el "principio de seguridad".
- Hacerlo requiere tener en cuenta aspectos como el análisis de riesgos, las políticas organizativas y las medidas físicas y técnicas.
- También debe tener en cuenta los requisitos adicionales sobre la seguridad de su tratamiento, que también son aplicables a los encargados del tratamiento de datos.
- Puede considerar el nivel tecnológico y los costes de aplicación a la hora de decidir qué medidas tomar, pero deben ser adecuadas tanto para sus circunstancias como para el riesgo que supone su tratamiento.
- Cuando sea apropiado, debe intentar utilizar medidas como la pseudonimización (por ejemplo, utilizando la protección de la privacidad con una máscara de desenfoque), y el cifrado.
- Sus medidas deben garantizar la "confidencialidad, integridad y disponibilidad" de sus sistemas y servicios y de los datos personales que trate en ellos.
- Las medidas también deben permitirle restablecer el acceso y la disponibilidad a los datos personales de manera puntual en caso de un incidente físico o técnico.
- También tiene que asegurarse de que dispone de los procesos adecuados para comprobar la eficacia de sus medidas y acometer las mejoras necesarias.

Anexo: Aviso en el lugar

Los avisos en el lugar deben incluir un pictograma (por ejemplo, el pictograma ISO o el pictograma utilizado habitualmente en el lugar donde se encuentra el edificio. El pictograma también debe ser comprensible para los niños. Puede encontrarlo, por ejemplo, en la página de símbolos gráficos ISO (https://www.iso.org/obp/ui/#search/grs/). El aviso debe:

- Identificar el responsable del tratamiento de datos
- Especificar el objetivo de la vigilancia:
    - Para que los organismos públicos realicen sus funciones
    - Ejercer el derecho a determinar a quién se le permitirá o denegará el acceso
    - Para garantizar los intereses legítimos para fines específicamente definidos
- Mencionar claramente si las imágenes son grabadas
- Proporcionar información de contacto y un enlace a la política de videovigilancia en línea
- Si alguna área fuera de los edificios está bajo vigilancia, esto debe indicarse claramente

El personal de seguridad y la recepción deben recibir formación sobre los aspectos de protección de datos de las prácticas de videovigilancia y deben poder hacer copias del aviso detallado de protección de datos (consulte Anexo: Política de videovigilancia en la página 49), disponible a petición. También deben poder comunicar a los miembros del público a quién dirigirse para hacer preguntas adicionales o para poder consultar sus datos.

Las señales deben estar ubicadas en esos lugares y ser lo suficientemente grandes como para que los titulares de los datos puedan advertirlas antes de entrar en el área vigilada y puedan leerlas sin dificultad. Esto no implica que deba colocarse un aviso junto a cada cámara.

Las señales dentro de los edificios deben estar en el idioma (o idiomas) que generalmente comprendan los miembros del personal y los visitantes más habituales. Las señales en el exterior de los edificios (si se vigilan las áreas exteriores) también deben estar escritas en el idioma (o idiomas) locales.

Para ver un modelo de notificación en el lugar de los hechos, consulte la plantilla*Milestone Aviso en el lugar*.

Anexo: Política de videovigilancia

La política de videovigilancia tiene muchos propósitos y sirve para satisfacer las siguientes necesidades:

- La adopción de este documento suele ser necesaria para completar y especificar la base jurídica y, por lo tanto, ayudar a establecer un motivo legal para la videovigilancia (consulte el artículo 5 del RGPD).
- Poner las prácticas por escrito y reflexionar sobre qué otras medidas adicionales hay que adoptar probablemente mejore los procedimientos y garantice un mejor cumplimiento.
- Adoptar una política y ponerla a disposición del público contribuirá a cumplir la obligación que impone el RGPD de proporcionar al público la información necesaria para garantizar un tratamiento justo.
- La política establece un conjunto de reglas cuyo cumplimiento puede medirse (por ejemplo, durante una auditoría).
- Aumentando la transparencia y demostrando los esfuerzos de cumplimiento, las organizaciones inducen la confianza en sus empleados y en terceros, y ayudan a facilitar las consultas con las partes interesadas.

La política de videovigilancia debe prever lo siguiente:

- Presentar una visión general del sistema de videovigilancia y describir sus propósitos
- Describir cómo funciona el sistema, cómo se utilizan los datos personales y qué garantías de protección de datos se han establecido
- Confirmar explícitamente el cumplimiento del RGPD
- Indicar las medidas necesarias para su implementación

Las organizaciones deben hacer públicas sus políticas de videovigilancia en sus sitios de intranet e Internet. Si este documento contiene información confidencial, debe hacerse pública una versión no confidencial.

Para poder servir como un aviso de protección de datos adecuado, la siguiente información debe integrarse en su política de videovigilancia en un lenguaje y formato fáciles de comprender:

- Identidad del responsable del tratamiento de datos (por ejemplo, organización, Dirección General, Dirección y unidad)
- Descripción breve de la cobertura del sistema de videovigilancia (por ejemplo, puntos de entrada y salida, salas de ordenadores, salas de archivos)
- La base jurídica de la videovigilancia, por ejemplo, el artículo 6 (1) (f) del RGPD
- Los datos recopilados y la finalidad de la videovigilancia (también deben especificarse claramente las limitaciones de los usos permitidos)
- Quién tiene acceso al material de vigilancia y a quién pueden revelarse las grabaciones
- Cómo se protege y garantiza la información
- Durante cuánto tiempo se guardan los datos
- Cómo pueden verificar, modificar o suprimir su información los interesados (incluida la información de contacto para otras preguntas e información sobre cómo obtener un recurso interno)

Además, la política de videovigilancia debe proporcionar referencias a:

- Los informes de auditoría de la organización
- Los informes de evaluación de impacto de la organización

Para obtener un modelo de política de videovigilancia, consulte la plantilla de*Milestone Política de videovigilancia*.

Limitación de responsabilidad: El modelo de política de videovigilancia debe ser comprobado por el responsable del tratamiento. El cumplimiento del RGPD con esta plantilla es su área de responsabilidad.

Tenga en cuenta que: la recopilación de audio y metadatos no está cubierta por el Sello Europeo de Privacidad. Una configuración de VMS con la recogida de audio y metadatos no tiene derecho a utilizar el perfil de producto certificado EuroPriSe. Un controlador / procesador de datos que lo haga no puede señalar que está utilizando un producto que facilita especialmente la protección de datos y el cumplimiento del RGPD.

Anexo: Evaluación del impacto de la protección de datos

Según el artículo 35 del RGPD, se requiere una *evaluación de impacto de la protección de datos* si la vigilancia

pudiera suponer un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del mismo, una evaluación del impacto de las operaciones de tratamiento previstas sobre la protección de los datos personales.

El controlador de datos debe consultar a la autoridad de supervisión antes del tratamiento cuando una *Evaluación de impacto de la protección de datos* en virtud del artículo 35 indica que el tratamiento daría lugar a un alto riesgo en ausencia de medidas adoptadas por el controlador de datos para mitigar el riesgo (Consulta previa, artículo 36 del RGPD).

Crear y mantener una *evaluación de impacto de la protección de datos*, un aviso a las personas afectadas. Este documento:

- Describe el objetivo de la vigilancia
- Es conservado por el controlador de datos o el procesador de datos
- Define la política de retención

Antes de instalar e implantar sistemas de videovigilancia se debe realizar una *evaluación del impacto de la protección de datos*, siempre que ello suponga un valor añadido a los esfuerzos de cumplimiento de la organización. El objetivo de la *evaluación de impacto sobre la protección de datos* es determinar el impacto del sistema propuesto sobre la privacidad de las personas y otros derechos fundamentales, así como identificar formas de mitigar o evitar cualquier efecto adverso.

Como mínimo, de acuerdo con el artículo 35 (7) del RGPD, la evaluación debe contener al menos:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, incluyendo, en su caso, el interés legítimo perseguido por el responsable del tratamiento
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en relación con los propósitos
- Una evaluación de los riesgos para los derechos y libertades de los titulares de los datos a los que se refiere el artículo 35 (1) del RGPD:

  > *Donde un tipo de tratamiento, en particular que utiliza nuevas tecnologías, y teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, pueda suponer un riesgo elevado para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de los datos personales. Una única evaluación puede referirse a un conjunto de operaciones de transformación similares que presentan riesgos elevados parecidos.*

- Las medidas previstas para hacer frente a los riesgos, incluidas garantías, medidas de seguridad y mecanismos para garantizar la protección de los datos personales y demostrar el cumplimiento del RGPD teniendo en cuenta los derechos e intereses legítimos de los interesados y otras personas afectadas

El esfuerzo que conviene invertir en una *evaluación de impacto de la protección de datos* depende de las circunstancias. Un sistema de videovigilancia con grandes riesgos inherentes, o que plantee cuestiones complejas o novedosas, justifica la inversión de un esfuerzo mucho mayor que uno con un impacto comparativamente limitado sobre la privacidad y otros derechos fundamentales, como un sistema convencional de CCTV estático operado con fines típicos de seguridad.

En cualquier caso y en todos los casos, ya sea en una *evaluación del impacto de la protección de datos* formal o de otro tipo, las organizaciones deben evaluar y justificar si recurren a la videovigilancia, cómo ubicar, seleccionar y configurar sus sistemas, y cómo aplicar las salvaguardias de protección de datos.

Además, puede haber casos en los que una organización proponga un sistema no estándar. En este caso, la organización debe evaluar cuidadosamente las diferencias previstas con respecto a la práctica y las recomendaciones, discutirlas con su responsable de protección de datos y con otras partes interesadas, y documentar su evaluación por escrito, ya sea en una *evaluación de impacto sobre la protección de datos* formal o de otro modo. La auditoría del sistema por parte de la organización también debe abordar la legalidad de la personalización del sistema.

Por último, debido a su complejidad, novedad, especificidad o riesgos inherentes, es muy recomendable realizar una *evaluación de impacto de la protección de datos* en los siguientes casos:

- Videovigilancia con propósitos distintos a la seguridad (incluso con propósitos de investigación)
- Videovigilancia de espacios públicos
- Monitorización de los empleados
- Monitorización en el territorio de los estados miembros y en terceros países
- Categorías especiales de datos
- Áreas con mayores expectativas de privacidad
- Videovigilancia de alta tecnología y/o inteligente
- Sistemas interconectados
- Grabación de audio

La *evaluación de impacto de la protección de datos* puede ser realizada internamente o por un contratista independiente. La evaluación debe realizarse en una fase temprana del proyecto. Basándose en los resultados de la *evaluación de impacto de la protección de datos*, una organización puede decidir:

- Abstenerse o modificar la monitorización prevista y/o
- Para implementar salvaguardas adicionales

Riesgos inherentes al uso del VMS

Al realizar la *evaluación de impacto de la protección de datos*, debe ser consciente de los riesgos inherentes al uso del VMS.

La *evaluación del impacto de la protección de datos* debe estar adecuadamente documentada. Como principio, un informe de *evaluación de impacto de la protección de datos* debe especificar claramente los riesgos para la privacidad y/u otros derechos fundamentales que la organización ha identificado, así como las salvaguardias adicionales propuestas. Tenga en cuenta los siguientes riesgos de vulneración de los derechos personales:

- Empresa/empleador, utilizando los vídeos, las alarmas o los registros de auditoría para:
  - Monitorizar las horas de trabajo de los empleados en el sitio investigado, por ejemplo, la hora de llegada y salida
  - Monitorizar la efectividad de los empleados controlando dónde pasan su tiempo, la cantidad de tiempo que pasan en la máquina de café, el tiempo que pasan en los baños, siempre y cuando trabajen efectivamente en la tarea que tienen
  - Monitorizar lo que el empleado está mirando en sus pantallas de ordenador
  - Monitorizar si los empleados cumplen los requisitos de trabajo o de seguridad, por ejemplo en los lugares de construcción
  - Mostrar grabaciones de vídeo de los empleados a otros empleados o gerentes para intimidar al empleado o amenazar a otros empleados para que hagan lo mismo
  - Verificar si los guardias/operadores de seguridad desempeñan sus funciones de forma eficaz, por ejemplo, comprobando si utilizan activamente a los clientes, seleccionando las cámaras, ejecutando las reproducciones, etc.
- Empresa/propietario/operador/vigilantes, utilizando vídeos para:
  - Compartir en las redes sociales grabaciones de vídeo de personas (empleados de la empresa o público en general) en situaciones embarazosas o delicadas
  - Utilizar cámaras PTZ para acercarse a las personas y obtener grabaciones íntimas / inapropiadas en primer plano de ellas sin su conocimiento
- Empresa/propietario/operador/vigilantes
  - Exportar vídeos o facilitar el acceso a vídeos grabados de forma no crítica a quien lo solicite

Fuentes adicionales para identificar el riesgo son:

- La *Milestone Guía para reforzar* proporciona el Marco de gestión de riesgos cibernéticos, que describe los seis pasos recomendados para categorizar, seleccionar, implementar, evaluar, autorizar y supervisar los riesgos. La *Milestone Guía para reforzar* la seguridad ofrece una serie de riesgos técnicos y recomendaciones para mitigarlos. Estos incluyen, pero no se limitan a la protección de la privacidad del VMS en términos de una serie de violaciones de datos y riesgos de acceso no autorizado por una configuración técnica débil, diseño y operaciones de mantenimiento. Para obtener más información sobre cómo asegurar sus instalaciones XProtect VMS ontra los ciberataques, consulte la guía para reforzar.
- La *Milestone Guía de privacidad* (esto) proporciona recomendaciones sobre la gestión de los riesgos operativos no técnicos, incluida la gestión de los derechos y las solicitudes de los interesados, las funciones y las responsabilidades de un VMS, las plantillas para la notificación in situ, la política de videovigilancia y los *Acuerdos de procesamiento de datos*.

- El Milestone aprendizaje electrónico sobre la privacidad de usuario final ofrece una formación de concienciación para las operaciones de VMS y a los supervisores sobre cómo, en el funcionamiento diario, manejar los riesgos de privacidad relacionados con el VMS. Vea más información en el Milestone sitio web de la certificación del RGPD.

Anexo: Acuerdo de procesamiento de datos

El controlador de datos debe tener un *Acuerdo de procesamiento de datos* con cualquier tercero con el que el controlador de datos comparta medios de videovigilancia, excepto para compartir medios de videovigilancia con las fuerzas del orden.

Si una organización subcontrata todas o parte de sus actividades de videovigilancia a un tercero (un procesador de datos), sigue siendo responsable del cumplimiento del RGPD como controlador de datos. Por ejemplo, guardias de seguridad que supervisan la videovigilancia en directo en la zona de recepción de una organización que trabaja para una empresa privada a la que la organización ha subcontratado la tarea de monitorización en directo. En este caso, la organización debe garantizar que los guardias de seguridad lleven a cabo sus actividades de conformidad con las disposiciones del RGPD.

Para ver un modelo de Acuerdo de procesamiento de datos, consulte la plantilla *Milestone Acuerdo de procesamiento de datos*.

Limitación de responsabilidad: La plantilla del *Acuerdo de procesamiento de datos* debe ser revisada por el responsable del tratamiento. El cumplimiento del RGPD con esta plantilla es su área de responsabilidad.

Anexo: El sistema Milestone XProtect VMS y el RGPD

Tenga en cuenta que: Esta sección describe los requisitos y las restricciones para ser un producto certificado con el Sello de Privacidad Europeo (EuroPriSe). Un responsable/encargado del tratamiento de datos que se desvíe de estos requisitos no puede señalar que él o ella está utilizando un producto que facilita especialmente la protección de datos y el cumplimiento del RGPD.

Componentes y dispositivos que no están cubiertos por el Sello Europeo de Privacidad

Los siguientes componentes y dispositivos no están cubiertos por el Sello Europeo de Privacidad:

- Plug-ins disponibles en marketplace Milestone
- Servidor XProtect Mobile (desactivado por defecto)
- Cliente XProtect Mobile
- XProtect Web Client

- XProtect Access (desactivado por defecto)
- XProtect LPR (desactivado por defecto)
- XProtect Transact (desactivado por defecto)
- Milestone Interconnect
- XProtect DLNA Server
- Milestone Open Network Bridge (integración segura de vídeo privado a público)
- XProtect Event Server plug-ins
- Tratamiento de los datos de audio (desactivado por defecto)
- Tratamiento de los metadatos (desactivado por defecto)
- Tratamiento de los datos de los dispositivos de entrada y salida (desactivado por defecto)
- XProtect BYOL como se proporciona por medio de https://aws.amazon.com/marketplace/pp/B089DKW36G

Para que la instalación de Milestone XProtect VMS esté cubierta por el Sello de Privacidad Europeo, estos componentes no deben ser instalados.

Además, el producto estándar no realiza reconocimiento facial, análisis de comportamiento, seguimiento automático o reconocimiento de personas en la transmisión en directo o en los medios grabados. Estas funcionalidades tampoco cumplen con el Sello de Privacidad Europeo.

Esto significa que cuando instala el XProtect VMS, no utiliza la opción de un **sólo ordenador** en el instalador, porque instala automáticamente el Mobile Server.

En su lugar, instala el sistema XProtect VMS con las opciones **Distribuido** o **Personalizado**. Esto no instala el Mobile Server.

Una vez que se haya instalado XProtect VMS la página de descarga en el Management Server listará los DLNA Server adicionales y los componentes Mobile Server. No instale estos servidores.

Guía de actualización

Si está actualizando una instalación de la versión de Milestone XProtect VMS 2018 R2 o anterior, los antiguos archivos de registro deben ser eliminados manualmente para que la instalación cumpla con el RGPD.

Después de haber actualizado el XProtect VMS, los antiguos archivos de registro pueden ser eliminados utilizando la información y la herramienta descrita en este artículo de Base de conocimientos.

Red segura para la autenticación y la transmisión de datos

Diseñe una infraestructura de red que utilice la red física o la segmentación VLAN en la medida de lo posible.

Milestone recomienda que seleccione cámaras que soporten HTTPS. Se recomienda configurar las cámaras en VLAN separadas y utilizar HTTPS para la comunicación entre la cámara y el servidor de grabación, así como para la comunicación entre los clientes y el servidor de grabación.

Se recomienda que XProtect Smart Client y XProtect Smart Wall están en la misma VLAN que los servidores.

Utilice una red cifrada VPN o similar si utiliza Smart Client o Smart Wall desde una ubicación a distancia.

Habilite la encriptación para todas las comunicaciones. Para obtener información sobre sus instalaciones XProtect VMS, consulte la guía para reforzar y la guía de certificados.

Tenga en cuenta que: El transporte no cifrado y no seguro de los datos de vídeo violaría el sello EuroPriSe y llevaría a la pérdida del cumplimiento del sello de privacidad EuroPriSe.

Enmascarar a personas en caso de acceso

Según el artículo 15 del RGPD, el titular de los datos tiene derecho a acceder a sus datos personales que están siendo procesados, por ejemplo, las grabaciones de vídeo del titular.

El titular de los datos tiene derecho a solicitar a una empresa información sobre qué datos personales (sobre él o ella) se están procesando y la justificación de dicho tratamiento.

Debido a que XProtect VMS no soporta la identificación automática de las personas, debe establecer medidas adicionales para garantizar los derechos de las personas. En el contexto del VMS, consulte Anexo: Aviso en el lugar en la página 48.

Más aún, XProtect VMS no soporta el enmascaramiento de otras personas que se desplazan y que están registradas junto con el demandante por el derecho de acceso.

En Milestone Marketplace se pueden encontrar varias soluciones de socios técnicos de Milestone para el desenfoque dinámico de todas u otras personas antes de la exportación. Como alternativa, se puede añadir el desenfoque a las imágenes individuales o a los flujos de vídeo de forma manual o asistida después de la exportación. Algunas empresas ofrecen el desenfoque como servicio (por ejemplo, FACIT Data Systems).

Eliminar parcialmente grabaciones de vídeo

Según el artículo 17 del RGPD, el titular de los datos tiene derecho a solicitar la supresión de sus datos. En el contexto del VMS, esto a menudo no se cumple debido a los intereses legítimos primordiales (detección de fraude, salud y seguridad) u otros fines empresariales indicados en la política de videovigilancia (consulte Derecho al olvido (Derecho a la supresión) en la página 36 y Anexo: Política de videovigilancia en la página 49). La política de videovigilancia define la conservación automática (por defecto, 7 días) que garantiza la eliminación automática de las grabaciones, y esto debe equilibrar de forma justa los derechos de los titulares de los datos frente a los propósitos empresariales razonables.

Si un titular de datos solicita la supresión de sus datos, se recomienda que el responsable del tratamiento utilice una *Solicitud del titular de datos* para documentar la reclamación (consulte Solicitud del titular de los datos en la página 11). Para ver un modelo de solicitud del titular de los datos, consulte la plantilla *Milestone Solicitud del titular de los datos*.

Debe eliminar todas las grabaciones de la cámara o cámaras en cuestión.

Para conservar todas las demás grabaciones que no deben ser eliminadas, exporte todos los datos y guárdelos de forma segura. No puede restaurar estos datos de vuelta al VMS.

Cualquier exportación debe estar cifrada y firmada digitalmente, y excluir los intervalos de tiempo especificados de la cámara o cámaras específicas. Es decir, exportar hasta la hora/fecha y exportar después de la hora/fecha. Esto puede dar lugar a copias de seguridad de múltiples periodos de tiempo.

El Smart Client – Player puede entonces ser usado para ver los datos.

Se recomienda que el responsable del tratamiento busque asesoramiento jurídico y lleve a cabo tanto una evaluación del impacto sobre el negocio como una evaluación del impacto sobre la privacidad (consulte Realización de una evaluación de impacto en la página 32) antes de ejecutar el derecho al olvido del titular de los datos, ya que la supresión puede introducir nuevos riesgos para el negocio que pueden inclinar la balanza de intereses e introducir riesgos que afecten negativamente a la protección de la privacidad de otros titulares de los datos.

Utilizar fondos geográficos en XProtect Smart Client

XProtect Smart Client soporta el uso de fondos geográficos. Estos fondos muestran los fondos de planos.

Se arriesga a violar el RGPD si utiliza cualquiera de los siguientes servicios de planos, y no cumplirá con el RGPD dentro de la certificación de EuroPriSe:

- Bing Maps
- Google Maps
- Milestone Map Service

Estos servicios no proporcionan las garantías adecuadas en relación con el tratamiento de los datos personales en los EE.UU. El cliente se convierte en el responsable (conjunto) del tratamiento de los datos del usuario.

Consulte cualquier actualización de la sentencia Schrems II por parte de la Comisión Europea en el sitio web oficial.

Como alternativa, se recomienda configurar el servicio privado **OpenStreetMap** para el fondo geográfico.

Integraciones de socios registrados

Cuando se activa una licencia, Milestone recopila datos "por integración". El XProtect VMS recoge datos sobre plugins y los fabricantes de plugins y sobre los plugins y la integración que el cliente utiliza.

Los datos que se recopilan de cada instalación son:

- Nombre de integración
- Fabricante de la integración
- Versión de integración

- Tipo de integración (independiente, Smart Client, Management Client, Event Server) y un número de instancias de cada tipo (es decir, cuántos clientes están ejecutando el plugin)

Los desarrolladores de plugins nunca deben utilizar nombres personales al registrar su producto. Utilice sólo el nombre de la empresa.

Los datos sólo se procesan por Milestone si el fabricante del plugin está incluido en el mercado y ha aprobado el tratamiento de los datos con el fin de mejorar Milestone XProtect Corporate (y no para la comercialización y la investigación de mercado). Si el plugin no se registra, los datos se eliminan inmediatamente. La base legal del procesamiento es el artículo 6 (1) (f) del RGPD, que muestra los intereses legítimos de Milestone y los usuarios del VMS.

Garantías adicionales

Para garantizar mejor que la configuración de Milestone XProtect VMS cumple con el RGPD, esta lista le ofrece algunas garantías adicionales que debe tener en cuenta al configurar el sistema.

Problema	Impacto negativo en la privacidad	Consejos para el responsable del tratamiento de datos
Las cámaras PTZ y el enmascaramiento de la privacidad no funcionan juntos. Los enmascaramientos no siguen las mociones de PTZ.	El efecto de mejora de la privacidad del enmascaramiento puede ser burlado.	Milestone recomienda que haga una de las siguientes cosas: • No debe utilizar la función de enmascaramiento de privacidad XProtect incorporada en las cámaras PTZ porque la máscara es estática en relación con los píxeles decodificados de la imagen y no con la dirección/ubicación real de la cámara PTZ. • Desactive la funcionalidad PTZ cuando utilice máscaras.

Problema	Impacto negativo en la privacidad	Consejos para el responsable del tratamiento de datos
		• Compre cámaras PTZ que admitan el enmascaramiento dinámico de la privacidad (de modo que las zonas seleccionadas siempre queden enmascaradas, independientemente de la ubicación y el zoom de la cámara).
El uso de micrófonos o dispositivos de metadatos puede atentar contra la intimidad personal. (En XProtect Corporate, están desactivados por defecto).	El uso de micrófonos puede violar fácilmente el cumplimiento del RGPD.  Tenga en cuenta que: Utilizar micrófonos y dispositivos de metadatos no está cubierto por el Sello Europeo de Privacidad. Su activación violaría el sello EuroPriSe.	Antes de activar los micrófonos o los dispositivos de metadatos, debe asegurarse de que tiene un propósito claramente justificado para la recogida de datos. Consulte ¿Tiene una base legal para recopilar datos? en la página 27
Los operadores y administradores pueden exportar o copiar los datos de vídeo, los archivos de vídeo, las copias de seguridad de la configuración y los registros de auditoría en discos duros locales o en soportes extraíbles como CD, DVD, unidades flash USB, etc.	Los datos personales salen de las fronteras de la gobernanza de XProtect VMS. Los datos ya no están protegidos por los mecanismos de control de acceso de XProtect VMS y no pueden ser eliminados por XProtect VMS cuando se alcanza el período de conservación. Esto conlleva el riesgo de que los datos se almacenen durante más tiempo del permitido, de que se utilicen para diferentes propósitos y de que se viole la confidencialidad de los datos.	Los responsables del tratamiento adoptarán medidas técnicas y organizativas para proteger los datos que salgan de los límites de XProtect VMS. Consulte Gestión de datos exportados en la página 19 para las posibles medidas a tomar.

Problema	Impacto negativo en la privacidad	Consejos para el responsable del tratamiento de datos
Los datos del registro de auditoría y otros datos personales no están cifrados por el producto antes de ser almacenados en las bases de datos SQL. Los administradores de la base de datos pueden acceder a los datos del registro de auditoría utilizando clientes de la base de datos. XProtect Corporate no pueden controlar o registrar este acceso.	Especialmente, los datos sensibles del registro de auditoría pueden ser revelados a usuarios no autorizados. Consulte Protección de los datos almacenados y transmitidos en la página 45. Para obtener más información sobre cómo asegurar sus instalaciones XProtect VMS ontra los ciberataques, consulte la guía para reforzar.	Haga lo siguiente: • Implemente un concepto de rol adecuado para la administración de la base de datos. • Limite el acceso a la base de datos sólo para el personal autorizado. • Si es posible, active el cifrado de la base de datos mediante mecanismos de base de datos.
El producto implementa una función de copia de seguridad. Esta función hace una copia de seguridad de la configuración del VMS pero no de la base de datos del registro de auditoría.	La destrucción física del soporte de datos que contiene la base de datos de los registros de auditoría podría impedir al responsable del tratamiento cumplir con sus obligaciones de rendición de cuentas cuando no existen copias de seguridad de los registros de auditoría.	Considere la posibilidad de crear copias de seguridad de la base de datos del registro de auditoría. Si el responsable de los datos decide crear copias de seguridad de la base de datos del registro de auditoría, también debe establecer un proceso para eliminar las copias de seguridad cuando se alcance el período de conservación y protegerlas contra el acceso no autorizado (por ejemplo, cifrando la copia de seguridad, poniendo bajo llave los medios de copia de seguridad, etc). Para obtener más información, consulte el manual de administrator para XProtect VMS.

Problema	Impacto negativo en la privacidad	Consejos para el responsable del tratamiento de datos
XProtect VMS utiliza una autenticación criptográfica no segura para algunas comunicaciones cliente-servidor y para algunas comunicaciones servidor-servidor / tokens de autorización a través de canales de comunicación no seguros.	Los atacantes con acceso a la red podrían espiar los tokens y utilizarlos para hacerse pasar por usuarios del VMS o por componentes del servidor. Esto podría comprometer la confidencialidad de los datos de vídeo o la integridad de todo el sistema. Tenga en cuenta que: La VPN y/o el HTTPS deben estar configurados para proteger las comunicaciones no seguras para cumplir con el sello EuroPriSe.	Haga lo siguiente: • Utilice unas VPN criptográficamente seguras. Para obtener más información sobre cómo asegurar sus instalaciones XProtect VMS ontra los ciberataques, consulte la guía para reforzar. • Redes separadas. Para obtener más información sobre cómo asegurar sus instalaciones XProtect VMS ontra los ciberataques, consulte la guía para reforzar. • Configure la dirección HTTPS para el Recording Server. Para obtener información sobre sus instalaciones XProtect VMS, consulte la guía para reforzar y la guía de certificados.
El funcionamiento de una VPN en modo dividido podría revelar la dirección IP privada de usuarios XProtect VMS.	Cuando se habilita el túnel dividido, los usuarios evitan la seguridad a nivel de puerta de enlace que pueda haber en la infraestructura de la red.	Haga lo siguiente: • Utilice una conexión VPN segura (una VPN es segura por defecto, pero algunos protocolos VPN antiguos no cifran los datos intercambiados entre el servidor y el cliente)

Problema	Impacto negativo en la privacidad	Consejos para el responsable del tratamiento de datos
		• Utilice siempre la tunelación completa • Utilice los protocolos de autenticación más compatibles (si los hay) • Utilice Active Directory para autenticar a los usuarios de la VPN Para obtener más información sobre cómo asegurar sus instalaciones XProtect VMS ontra los ciberataques, consulte la guía para reforzar.
El producto permite establecer tiempos de retención para registros de auditoría, datos de vídeo, alarmas y otros datos personales.	Establecer el tiempo de conservación en períodos demasiado largos podría violar los requisitos del RGPD en cuanto a las limitaciones de almacenamiento (artículo 5 (1)(e) y artículo 17 del RGPD).	Los tiempos de conservación deben adaptarse a los propósitos del tratamiento (consulte Derecho al olvido (Derecho a la supresión) en la página 36).
Los administradores pueden configurar los destinatarios del correo electrónico que pueden recibir fragmentos de vídeo o imágenes fijas del VMS cuando se producen determinados eventos. No es posible configurar una lista blanca de dominios permitidos para estos destinatarios de correo electrónico.	Un error tipográfico podría dar lugar a una violación de datos cuando un tercero reciba correos electrónicos con datos de vídeo y alarmas del sistema.	Haga que el responsable del tratamiento sea consciente de este riesgo. Milestone recomienda que establezca un proceso organizativo, como el principio de los cuatro ojos, que reduce el riesgo de fallos al introducir las direcciones de correo electrónico.

Problema	Impacto negativo en la privacidad	Consejos para el responsable del tratamiento de datos
Las notificaciones son correos electrónicos que se envían a una dirección de correo electrónico determinada. Al crear una notificación, el administrador puede decidir incluir un conjunto de instantáneas o un AVI de una secuencia.	Debido a que las instantáneas adjuntas y las secuencias AVI en las notificaciones salen del VMS, están fuera del control del VMS para el acceso y la retención del usuario.	Como los mensajes de correo electrónico y su contenido salen del control de acceso y conservación del usuario del VMS, se recomienda no adjuntar imágenes o secuencias AVI a notificaciones de correo electrónico. Si el cliente necesita esta característica, al menos debe asegurarse de que existen procedimientos y controles organizativos sobre quién recibe los correos electrónicos y cómo se gestionan. Consulte Tratamiento de los datos exportados en las notificaciones y el correo electrónico en la página 21.

Anexo: Procesamiento de datos en el entorno de Milestone XProtect VMS

El *Milestone documento de arquitectura de sistema* describe los componentes del sistema y la forma en que interactúan entre sí y con los componentes del sistema del entorno. Para cada uno de los casos de uso relevantes del producto, encontrará un diagrama que ilustra el flujo de comunicación entre los componentes que intervienen en los casos de uso. Estos diagramas ofrecen una visión general de los datos transferidos. Para obtener información sobre cómo los componentes del Milestone XProtect VMS, consulte el documento Milestone que describe la arquitectura del sistema.

Esta sección enumera los procesos de instalación por defecto de los datos personales, autenticación y configuración de XProtect que son relevantes para los ajustes de privacidad y seguridad.

Datos personales del VMS

El principal tipo de datos son los datos de vídeo de las cámaras de vídeo. Estos datos son almacenados por el servicio de Recording Server. Los datos de vídeo pueden transmitirse en directo o en modo de reproducción a XProtect Smart Client. El otro dato son los datos maestros de los usuarios del VMS que se almacenan en la base

de datos SQL.

Datos personales del entorno

Los datos personales de los usuarios del VMS provienen del entorno Windows donde se utiliza Active Direct (AD) para la autenticación de los usuarios y como fuente para la pertenencia a grupos. Las consultas de servicio de Milestone XProtect Management Server en AD a través del protocolo LDAP para obtener información sobre los usuarios que se conectan al sistema.

Datos personales del sistema

Estos datos personales abarcan todo tipo de datos necesarios para asegurar, configurar, operar, mantener o dar soporte al sistema. Los tipos de datos personales incluyen:

- Datos de registro

  Los sistemas de TI suelen registrar los datos del usuario y del sistema en archivos de registro de auditoría y depuración para ayudar a operar y mantener los sistemas. XProtect Corporate también lo hace. El VMS registra información acerca de la mayoría de las acciones del usuario en la base de datos SQL. Este registro de auditoría se utiliza para comprender la responsabilidad de las acciones pasadas y el comportamiento del sistema y para rastrear el uso indebido del sistema. Los archivos de registro de depuración se utilizan para identificar defectos y fallos en el sistema. Los datos de depuración pueden contener o no datos personales.

  Las entradas de registro y los datos de depuración pueden revelar información detallada sobre el uso del sistema por parte de operadores y administradores y pueden ser adecuados para monitorizar el comportamiento y el rendimiento de los empleados.

- Registro de autenticación

  El servidor de autorización de Duende OAuth y Identity Provider (IDP) crea archivos de registro de auditoría con datos personales en el nodo del servidor que está ejecutando el IDP.

  El registro se realiza cuando:

  - Un usuario cambia la contraseña
  - Inicio de sesión fallido
  - Bloqueado por exceder el número de intentos permitidos para iniciar la sesión correctamente
  - Inicio de sesión correcto

  El archivo de registro está almacenado en \\ProgramData\Milestone\IDP\Logs\idp-audit.log.

  El archivo de registro es accesible sólo para el usuario de IIS y los administradores locales. Si el usuario de IIS cambia, estos permisos deben ser actualizados.

  Por defecto, los registros tienen un ciclo de 24 horas y se eliminan después de 30 días. El ajuste del registro es configurable en el archivo NLog.config.

Datos de autenticación y autorización

- Autenticación de usuario en el VMS

  Hay dos opciones para autenticar a los usuarios de VMS de XProtect Management Client y XProtect Smart Client. Puede utilizar los mecanismos de inicio de sesión de Windows o la autenticación nativa de VMS.

  En un entorno de Active Directory de Windows, puede configurar para utilizar el mecanismo de inicio de sesión integrado de Windows. La autenticación con el inicio de sesión de Windows se basa por defecto en el protocolo Kerberos. Esta es la opción más segura. En entornos heredados, es posible que los controladores de dominio no admitan Kerberos. En este caso, el inicio de sesión de Windows recurre automáticamente al protocolo NT Lan Manager (NTLMv2), que se considera menos seguro que Kerberos.

  En entornos sin controlador de dominio de Windows, puede utilizar el método de autenticación nativo de XProtect, que es la autenticación básica con ID de usuario y contraseña contra el SQL Server o la autenticación de Windows para grupos de trabajo, si está disponible.

  Por lo tanto, existen tres tipos de credenciales de autenticación:

  - Tokens de inicio de sesión de Windows (tokens Kerberos o NTLM)
  - Credenciales de autenticación básica
  - Autenticación de Windows para grupos de trabajo

  Después de una autenticación correcta, el usuario se registra en el VMS y el servicio Management Server crea una sesión de usuario, donde se produce el inicio de sesión. Ahora el cliente puede acceder a la funcionalidad del servicio Management Server en el contexto de esta sesión de usuario. Cuando el usuario quiere acceder a la funcionalidad en el servicio Recording Server, el XProtect Smart Client necesita también una sesión de usuario con este servicio de servidor.

- Autenticación de usuario en el servicio Recording Server

  Dado que la sesión de usuario entre el XProtect Smart Client / XProtect Management Client y el servicio Management Server no puede ser reutilizada para acceder al Recording Server, el Recording Server también necesita autenticar al usuario. Para autenticarse en el servicio Recording Server, el servicio Management Server proporciona al cliente un token de autenticación, que el cliente debe presentar al servicio Recording Server. Al mismo tiempo, el servicio Management Server envía el token de autenticación a todos los servicios Recording Server de la instalación VMS. A su vez, éstos pueden utilizarse para autenticar a los usuarios posteriormente.

  XProtect VMS utiliza un GUID simple como token de autenticación, que el cliente envía al servicio Recording Server. Los GUID son creados y gestionados por el servicio Management Server, que renueva estos tokens tras un periodo especificado. El GUID es simplemente un identificador del usuario en la base de datos SQL Server.

  > Tenga en cuenta que: Estos tokens no se transmiten de forma criptográficamente segura por el VMS y esto requiere salvaguardas adicionales en la capa de red del entorno. Consulte Garantías adicionales en la página 58 para obtener detalles y Anexo: El sistema Milestone XProtect VMS y el RGPD en la página 54 para información relativa a redes seguras.
  > Es importante que realice estos pasos adicionales para asegurarse de que tiene un producto que cumple con EuroPriSe.

- Datos de autorización

  Los datos de autorización para los usuarios de VMS se almacenan en la base de datos SQL en un SQL Server. En el momento de la puesta en marcha, los servicios Management Server y Recording Server extraen de la base de datos SQL los datos de autorización pertinentes, incluidos los tokens de autenticación para todos los usuarios, con el fin de estar preparados para el posterior acceso de los usuarios a los servidores. Cuando un administrador cambia los permisos o los roles o cualquier otra cosa que afecte a la autorización del usuario, esta actualización es almacenada por el servicio Management Server en la base de datos SQL en el SQL Server y también se propaga activamente a todos los servicios Recording Server. Los servicios Recording Server almacenan localmente los datos de autorización de los usuarios y todos los tokens de autenticación y, por tanto, pueden autenticar inmediatamente a los usuarios clientes que presenten su token de autenticación.

- Datos de configuración

  Aparte de ver datos que se establecen por el XProtect Smart Client, todos los datos de configuración para el sistema VMS se configuran a través del XProtect Management Client del VMS y se almacenan en la base de datos SQL. Existen diferentes tipos de datos de configuración:

  - Ajustes y preferencias del usuario
  - Permisos de usuario
  - Configuración del servidor
  - Ajustes del sistema
  - Configuración de la cámara y del dispositivo

  Aunque los datos de configuración no contengan datos personales, pueden afectar a la forma en que el VMS procesa los datos personales. Sólo para la evaluación, la información de autorización y los ajustes de seguridad y privacidad entre los datos de configuración enumerados anteriormente son relevantes.

helpfeedback@milestone.dk

Acerca de Milestone

Milestone Systems figura entre los proveedores más destacados de software de gestión de vídeo de plataforma abierta, tecnología que ayuda a determinar cómo garantizar la seguridad, proteger activos y aumentar la eficiencia empresarial. Milestone Systems da soporte a una comunidad de plataforma abierta que fomenta la colaboración y la innovación en el desarrollo y uso de tecnologías de vídeo en red, gracias a soluciones fiables y escalables de eficacia probada en más de 150 000 instalaciones de todo el mundo. Milestone Systems se fundó en 1998 y es una empresa independiente dentro del Canon Group. Para obtener más información, visite https://www.milestonesys.com/.