Videovigilancia y Protección de Datos

V. 3.0
Febrero 2024

SEGURIDADE A1

INTRODUCCIÓN

Este documento tiene por finalidad el servir de base y ayuda a la hora del cumplimiento de los deberes en materia de protección de datos intrínsecos a las entidades que cuenten con algún servicio o sistema de videovigilancia proporcionado por Sistemas de Seguridade A1 en sus instalaciones.

La normativa base de aplicación es:

- Reglamento UE 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (norma directamente aplicable).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales.

SEGURIDADE A1

Este manual ha sido elaborado como mecanismo de ayuda, no pretende sustituir las recomendaciones que su entidad pueda recibir o haya recibido de sus asesores en materia de protección de datos, ni tiene un contenido exhaustivo.

PREGUNTAS FRECUENTES

¿Es necesario que la entidad actualice su registro de actividades de tratamiento?

Sí, las entidades que dispongan de un sistema de videovigilancia deben crear la preceptiva actividad de tratamiento "videovigilancia" para incluirla en su RAT (Registro Actividades de Tratamiento).

¿Qué información debe incluir la actividad de tratamiento "videovigilancia"?

La actividad de tratamiento debe incluir la siguiente información:

- **El nombre y los datos de contacto del responsable** y, en su caso, del corresponsable, del representante del responsable y, **de ser pertinente, el del delegado de protección de datos.**
- Los **fines del tratamiento.**
- Una descripción de las **categorías de interesados** y de las **categorías de datos personales**
- Las **categorías de destinatarios** a quienes se comunicaron o comunicarán los datos personales, incluyendo los destinatarios en terceros países u organizaciones internacionales.
- En su caso, las **transferencias internacionales** de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional, así como la documentación sobre garantías adecuadas para determinados casos
- Los **plazos de conservación** de las imágenes.
- Y, cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad que el responsable aplique para garantizar la integridad y confidencialidad de los datos.

¿Qué es una evaluación de impacto en materia de protección de datos?

Se trata de una herramienta de carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

Cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, una evaluación de impacto de las actividades de tratamiento en la protección de datos personales.

¿La instalación y utilización del sistema de videovigilancia requiere habilitar medidas de seguridad y protocolos?

Sí, junto a la creación de la actividad de tratamiento, en virtud del artículo 32 del RGPD la entidad debe aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, definiéndolas en función del estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento.

Por riesgo deben entenderse todos aquellos activos que generen probabilidad y gravedad para los derechos y libertades de las personas físicas en lo que respecta a sus datos personales.

En su caso, fruto del Análisis de Riesgos o de la Evaluación de Impacto se implementarán en la entidad las medidas de seguridad que se establezcan para minimizar los riesgos.

¿La entidad responsable debe informar sobre la instalación y uso del sistema de videovigilancia?

Sí, la entidad responsable está obligada a informar de su instalación y uso.

Es importante tener en cuenta que, en el supuesto de la videovigilancia, debemos distinguir entre la información a proporcionar a personas empleadas, socios y, en su caso, voluntarios (dependiendo de la entidad), de la información a transmitir a la ciudadanía en general (visitantes que acceden a las instalaciones o clientes, por ejemplo).

Derecho de información al personal laboral en los sistemas de videovigilancia:

Se establece la obligación expresa de notificar a todo el personal laboral la existencia y/o instalación de los sistemas de vigilancia mediante cámaras, así como su finalidad y los derechos que le amparan.

Se recomienda que dicha información sea entregada por escrito, quedándole constancia fehaciente a la entidad de que las personas trabajadoras han recibido dicha información (firma de la misma en un documento informativo, acuse de recibo en un correo electrónico…)

Derecho de información en general:

La Agencia Española de Protección de Datos exige la instalación de carteles informativos de la existencia de cámaras de videovigilancia.

Por lo tanto, en el caso de la ciudadanía en general, nos encontramos con dos necesidades:

1ª.- El cartel informativo básico.

2ª.- A disposición en todo momento, bajo solicitud de cualquier persona interesada, la actividad de tratamiento, donde se deben especificar la base legitimadora, las finalidades, las posibles comunicaciones de datos, las categorías de datos recabados, el plazo de conservación y un resumen de las medidas de seguridad aplicadas por la entidad para garantizar la seguridad de los datos recabados a través de la videovigilancia, tal y como exige el artículo 13 del RGPD.

¿Qué información debe contener el cartel de aviso de cámaras de videovigilancia?

El contenido mínimo del cartel será:

Responsable: los datos del responsable del tratamiento (nombre, dirección, identificación fiscal…).

Derechos de protección: se debe indicar cómo pueden ejercer las personas sus derechos de protección de datos (cómo acceder, rectificar, cancelar, limitar el tratamiento…).

Delegado de Protección de Datos: en su caso, datos de contacto del DPD.

Información Adicional: facilitar la remisión a las personas interesadas a un correo electrónico, departamento o dirección en la que pueda solicitar toda la información relativa a la actividad de tratamiento.

La propia Agencia dispone a modo de ejemplo de un modelo descargable de dicho cartel en el siguiente link:

https://www.aepd.es/es/documento/cartel-videovigilancia.pdf

¿Dónde se deben colocar el cartel informativo? ¿Es necesario colocarlo debajo de cada cámara?

El cartel se debe exhibir en lugar visible y, como mínimo, en los accesos a las zonas vigiladas, ya sean interiores o exteriores. En caso de que el espacio videovigilado disponga de varios accesos, deberá disponerse de dicho distintivo de zona videovigilada en cada uno de ellos.

El Gabinete Jurídico de la Agencia Española de Protección de Datos se ha pronunciado respecto de la ubicación del cartel informativo, explicitando que "*no es necesario que se coloque debajo de la/s cámara/s, sino que será suficiente colocar el distintivo informativo en lugar suficientemente visible, tanto en espacios abiertos como cerrados. Por tanto, resultaría aconsejable que si tratándose de un edificio sometido a videovigilancia, en la entrada del mismo, se ubicara el cartel informativo*".

¿Qué derechos pueden ejercer las personas en relación con el sistema de videovigilancia?

Si bien los artículos 15 a 22 del RGPD regulan la totalidad de los derechos que los interesados pueden ejercitar (acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y oposición a decisiones individuales automatizadas) el ejercicio de estos derechos debe ser matizado en el ámbito de la videovigilancia.

La Agencia Española de Protección de Datos se ha pronunciado al respecto:

En primer lugar, no resulta posible el ejercicio del derecho de rectificación, ya que por la naturaleza de los datos (imágenes tomadas de la realidad que reflejan un hecho objetivo) se trataría del ejercicio de un derecho de contenido imposible.

En segundo lugar, tampoco sería aplicable el derecho de portabilidad, ya que, aunque se trata de un tratamiento automatizado, la legitimación no se basa ni en el consentimiento ni en la ejecución de un contrato.

En tercer lugar, no se aplicaría parte del contenido del derecho a la limitación del tratamiento, en su aspecto de "cancelación cautelar", que está vinculada al ejercicio de los derechos de rectificación y oposición.

Por otra parte, sí serían aplicables los siguientes derechos:

- El **derecho de acceso**, si bien este reviste características singulares, la que requiere aportar como documentación complementaria una imagen actualizada que permita al responsable verificar y contrastar la presencia del afectado en sus registros. Resulta prácticamente imposible acceder a imágenes sin que pueda verse comprometida la imagen de un tercero. Por ello, puede facilitarse el acceso mediante escrito certificado en el que, con la mayor precisión posible, y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.
- El **derecho de supresión**, con independencia del plazo máximo de un mes de supresión de las imágenes.
- El **derecho a la limitación del tratamiento**, que se aplicaría en su otra vertiente, es decir, se solicite al responsable que se conserven las imágenes cuando:
    - El tratamiento de datos sea ilícito y el interesado se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso.
    - El responsable ya no necesite los datos para los fines del tratamiento pero el interesado si los necesite para la formulación, ejercicio o defensa de reclamaciones.

¿Qué es un Encargado de Tratamiento?

El encargado del tratamiento es aquella entidad que realiza parte del tratamiento de los datos bajo las instrucciones y contrato del responsable de seguridad. En este supuesto, Sistemas de Seguridade A1, SL, es encargado del tratamiento del sistema de videovigilancia instalado en su organización.

El Considerando 81 del RGPD establece que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del RGPD, incluida la seguridad del tratamiento.

Sistemas de Seguridade A1, SL garantiza que cumple escrupulosamente con la normativa impuesta por el Reglamento Europeo de Protección de Datos, cumpliendo con lo establecido en el Considerando 81 antes mencionado.

Asimismo, el artículo 28 del RGPD exige que el tratamiento de los datos por parte del Encargado del Tratamiento se rija por un contrato que vincule al encargado respecto del responsable, estableciendo el contenido mínimo del mismo.

En dicho contrato, elaborado por el responsable del tratamiento, impondrá las instrucciones, obligaciones con respecto al tratamiento de los datos a Sistemas de Seguridade A1, SL, así como los permisos del tratamiento que concede a nuestra entidad.

Sistemas de Seguridade A1, SL se ofrece a la firma de cuanto contrato o anexo precise para el cumplimiento de su obligación, así como al pleno sometimiento del mismo.

¿La entidad responsable del sistema de videovigilancia puede facilitar datos a terceros?

La entidad está legitimada para comunicar las imágenes captadas sin consentimiento a los jueces y tribunales así como a las Fuerzas y Cuerpos de Seguridad.

La base de legitimación para los jueces y tribunales está recogida en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y a las Fuerzas y Cuerpos de seguridad, por el antiguo artículo 22 de la LOPD.

La petición de las grabaciones por parte de las Fuerzas y Cuerpos de Seguridad debe ser proporcional a la finalidad del requerimiento realizado, sin que se produzca una comunicación indiscriminada. A este respecto el artículo 22.2 de la LOPD establece que "*la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un* ***peligro real*** *para la seguridad pública o para la represión de infracciones penales…*".

La Agencia Española de Protección de Datos en reiterados informes ha venido a interpretar este artículo (informe 16 julio 1999, 213/2004, 0297/2005, 0145/2007, entre otros), considerando que el tratamiento de datos por parte de las Fuerzas y Cuerpos de Seguridad será posible siempre y cuando se cumplan los siguientes requisitos:

- Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.
- Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.
- Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.
- Que, en cumplimiento del artículo 22.4 de la LOPD, los datos sean cancelados cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

CONCLUSIÓN: sólo se puede ceder cuando la solicitud, que según sentencia del TC 14/2003, de 30 de enero, debe contener justificación razonada en la recogida y tratamiento de datos de carácter personal para fines policiales, se refiere a un caso concreto.

En cuanto a la solicitud de las imágenes por parte de particulares, para conocer la identidad de un tercero, a los efectos de poder ejercitar determinadas acciones judiciales y/o contractuales, para poder hacerse efectiva debe reunir los siguientes requisitos:

- Legitimación: el interés legítimo invocado por el particular debe referirse al ejercicio del derecho fundamental a la tutela judicial efectiva, en la medida que las imágenes se utilizarán para la obtención de pruebas para formular una posterior denuncia por delito, o reclamación por responsabilidad contractual, o extracontractual a una compañía de seguros
- Finalidad compatible: esta comunicación de datos no persigue una finalidad diferente con la que se recogieron los datos, pues entra dentro del término amplio de "seguridad".
- Minimización de datos: la cesión debe limitarse al mínimo necesario para la finalidad pretendida, en la medida que el solicitante pueda determinar exclusivamente lo relacionado con el incidente concreto a que se refiere su petición.

En todo caso, como responsable del tratamiento que es su entidad, de conformidad con la Ley de Enjuiciamiento Criminal, debe ser la organización quien de traslado del presunto delito a las autoridades competentes.

A este respecto se ha pronunciado en numerosas ocasiones la Agencia Española de Protección de Datos, llegando a recomendar en algunos supuestos que sea directamente la organización la que de traslado de las imágenes a las autoridades sin comunicar los datos al presunto responsable cuando la causa de los daños fuera delictiva.

Recomendamos la lectura de la respuesta a una consulta planteada a esta respecto por el Gabinete jurídico de la Agencia Española de Protección de Datos:
https://www.aepd.es/media/informes/informe-juridico-rgpd-interes-legitimo.pdf

¿La entidad tiene la obligación de designar qué personas tienen acceso a las imágenes?

La entidad responsable del tratamiento deberá designar las personas concretas que van a tener acceso a las imágenes que constarán como personas usuarias autorizadas en el documento del Análisis de Riesgos. Previamente deberán ser informadas y aceptar por escrito sus respectivas responsabilidades.

¿Existe un plazo máximo de conservación de las imágenes?

La normativa prevé un tiempo máximo en el que pueden guardarse las imágenes de un sistema de videovigilancia en 30 días; por tanto, no se excluyen periodos de conservación inferiores al máximo.

Aunque existen causas especiales que pueden prolongar ese periodo. Por ejemplo, si hay una investigación policial o judicial en curso, el tiempo de almacenamiento se extenderá a la duración de esta.

RESUMEN OBLIGACIONES RELACIONADAS CON LAS CÁMARAS

Las obligaciones mínimas que debe de cumplir una entidad al contar con un sistema de videovigilancia serán las siguientes:

- Colocación en lugares visibles de las instalaciones de placas de aviso para informar a las personas usuarias de la existencia de un sistema de videovigilancia. El cartel indicará de forma clara la identidad del responsable del tratamiento, ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos y dónde obtener más información sobre el tratamiento de los datos personales.

- Notificar por escrito a todo el personal de la entidad de que los espacios de trabajo tienen instalado un sistema de videovigilancia.

- Disponer de documento informativo sobre el uso de videocámaras a disposición de las personas usuarias que lo soliciten.

- Las imágenes captadas por las cámaras se limitarán al espacio de que se trate, salvo que sea imprescindible para la finalidad perseguida. No podrán captarse imágenes de la vía pública a excepción de una franja mínima de los accesos al establecimiento. Tampoco podrán captarse imágenes de terrenos y viviendas colindantes o de cualquier otro espacio ajeno. Si se utilizan cámaras orientables y/o con zoom, será necesaria la instalación de máscaras de privacidad para evitar captar imágenes de la vía pública, terrenos y viviendas de terceros.

- Las cámaras sólo captarán imágenes de los espacios indispensables para esta finalidad. En ningún caso se ubicarán en zonas de vestuarios, baños y espacios de descanso de las personas trabajadoras.

- El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido. A las imágenes grabadas accederán sólo las personas autorizadas que deberán introducir un código de usuario y una contraseña personal e intransferible.

- Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación, transcurrido el cual se procederá a su total destrucción, salvo las excepciones previstas por la normativa.

SEGURIDAD A1