OBLIGACIONES EN MATERIA DE VIDEOVIGILANCIA

Introducción

El uso de dispositivos de videovigiliancia, como cámaras o fotodetectores permiten la captación y en su caso grabación de imágenes (tanto de interiores, como de exteriores). Cuando estos dispositivos obtienen imágenes o la voz de personas identificadas o identificables constituye un dato de carácter personal a efectos de la aplicación de la normativa de protección de los datos de carácter personal.

En este apartado de la web, hemos recogido las preguntas más frecuentes que nos han planteado los clientes en relación a las obligaciones y limitaciones que se deben tener en cuenta a la hora de instalar hacer uso del sistema de seguridad.

Toda la información que aparece en este apartado tiene su origen en documentación publicada por la Agencia Española de Protección de Datos (en adelante, Agencia). No obstante, este portal web no tiene carácter oficial, ni vinculante, y por ello, todo lo que aquí se indica debe entenderse siempre a modo informativo, debiendo el cliente, siempre y en todo caso, acudir a los canales oficiales dispuestos por la Agencia para solventar cualquier cuestión que le pueda surgir al respecto, como por ejemplo, la guía sobre videovigilancia publicada en el año 2009, que puede encontrar en su página web (www.agpd.es).

1 ¿Qué es la Videovigilancia?

La videovigilancia permite la captación, y en su caso la grabación, de información personal en forma de imágenes. Cuando su uso afecta a personas identificadas o identificables esta información constituye un dato de carácter personal a efectos de la aplicación de la normativa de protección de datos.

2 ¿En qué me afecta?

En caso de que su sistema de seguridad capte, grabe, transmita, conserve o almacene imágenes o sonidos de personas identificadas o identificables, serán de aplicación los principios vigentes en materia de protección de datos personales, lo que puede conllevar consigo una serie de obligaciones (Ver pregunta nº3).

Algunos de los dispositivos de seguridad de Securitas direct permiten la captación y/o grabación de imágenes, entre ellos:

Fotodetectores (o fotoperimetrales)

Videodetectores

Cámaras

3 ¿Qué obligaciones me pueden surgir?

Antes de abordar una por una las obligaciones, es necesario distinguir entre:

Un Sistema de seguridad instalado en un hogar.

En este supuesto, al tratarse de sistemas a través de los cuales se captan imágenes en el ámbito personal y doméstico, entendiendo por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar no resultan de aplicación las obligaciones previstas en la normativa de protección de datos de carácter personal.

Debe tenerse en cuenta, no obstante, que esta excepción no aplicaría en caso de que su vivienda sea el lugar de trabajo de alguna otra persona (por ejemplo, empleados de hogar, cuidadores, etc.). En este caso, si deberá atenerse a las obligaciones que se detallarán a continuación.

Un sistema de seguridad está instalado en una empresa / negocio.

Si su sistema de seguridad está instalado en un local comercial, nave, oficina, o cualquier otro lugar en el que se desarrolle una actividad comercial, a continuación, dejamos reflejadas las obligaciones comunes de aplicación cuando se instala un sistema de videovigilancia, y que están dispuestas en la normativa de protección de datos de carácter personal.

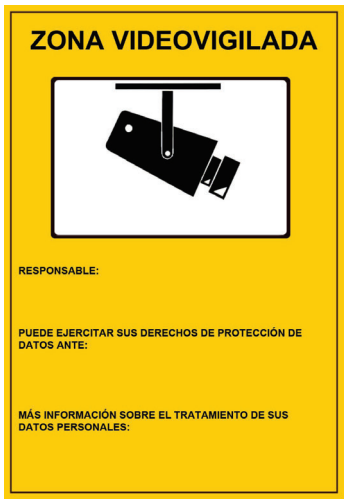
Tenga en cuenta que pueden existir otros requisitos u obligaciones adicionales en función de la finalidad y el tipo de instalación.

3.1 Deber de información – Distintivo de videovigilancia

Deberá informar obligatoriamente de la actividad de videovigilancia realizada en su local o negocio mediante un distintivo que contenga la información requerida en la normativa de protección de datos. El distintivo se ubicará como mínimo en los accesos a las zonas vigiladas, sean estos exteriores o interiores. Debe tenerse en cuenta que si el lugar vigilado dispone de varios accesos se debe colocar en todos ellos al objeto de que la información sea visible con independencia de por donde se acceda. Puede descargar el modelo de la Agencia de protección de datos accediendo a la web de la AEPD (www.aepd.es

En el recuadro en blanco, deberá de inscribir la dirección (electrónica o física) a través de la cual los afectados puedan ejercitar ante usted, los derechos de protección de datos conferidos por la normativa.

Para más información al respecto de los derechos a los que se hace relación en este apartado le recomendamos que pinche aquí, o bien, que consulte través del canal del responsable, en la propia web de la Agencia



3.2 Deber de información – Cláusula informativa

Como responsable del sistema de seguridad, además del distintivo de videovigilancia comentado en el punto 3.1, deberá disponer de un impreso con toda la información legalmente necesaria con posibilidad de imprimirlo a petición de los afectados.

Dicho impreso deberá informar al menos sobre:

- La existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En la web de la Agencia dispone de un modelo de dicha cláusula que puede descargarse directamente de la web.

3.3 Inventario de Tratamientos

Si usted accede y/o almacena cualquier imagen/grabación/voz procedente de su sistema de seguridad en sus propios sistemas, plataforma o herramientas (p.e. su PC), deberá disponer en todo momento de un inventario de actividades de procesamiento de datos debidamente actualizado donde se recoja este tratamiento de datos.

3.4 Acuerdo de acceso a datos

Sin perjuicio de que Securitas Direct España, S.A.U. es responsable del tratamiento de los datos personales recogidos para la correcta prestación de servicios, así como de las imágenes obtenidas como consecuencia de los saltos de alarma. Todo ello se regula en las condiciones generales de servicio del contrato de seguridad firmado por el cliente al comenzar la prestación del servicio.

No obstante, será necesario firmar un acuerdo de acceso a datos entre la empresa de seguridad y el cliente cuando exista la posibilidad de que la empresa de seguridad acceda a las imágenes en un escenario distinto al indicado en el párrafo anterior. Puede solicitar dicho acuerdo a través de la dirección dpo@securitasdirect.es.

Securitas Direct España, S.A.U. no accede, ni almacena las imágenes procedentes de los sistemas de seguridad más allá de los derivados de saltos de alarma, limitándose a la instalación y/o mantenimiento técnico de los equipos y sistemas de seguridad, por lo que, salvo que se produzca lo indicado en el párrafo anterior, no sería necesario la firma de dicho acuerdo de acceso a datos.

3.5 Medidas de seguridad

Como responsable de la instalación, el cliente debe cumplir con el deber de garantizar la seguridad de las imágenes según establece la normativa de protección de datos. Por ello, debe asegurarse de adoptar todas las medidas que sean necesarias para garantizar la seguridad de las imágenes, evitando su pérdida, alteración, acceso y/o tratamiento no autorizados.

Para determinar las medidas de seguridad aplicables, el cliente deberá evaluar el nivel de seguridad requerido, teniendo en cuenta el tipo de datos objeto de tratamiento, su contenido y la finalidad del tratamiento. Cualquier persona que tenga acceso a los datos debido a sus funciones, deberá observar la debida reserva, confidencialidad y sigilo en relación a los mismos.

Es obligación del cliente informar a cualquier persona que tenga acceso a los datos sobre sus obligaciones de seguridad y sobre su deber de secreto.

3.6 Cancelación de imágenes obtenidas

Las imágenes obtenidas por su sistema de seguridad deberán cancelarse en el plazo máximo de 30 días desde su captación. Una vez transcurrido ese plazo las imágenes deberán ser canceladas, lo que implica el bloqueo de las mismas. Se conservarán únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales que las requieran oficialmente, y durante el plazo de prescripción de éstas. Una vez cumplido dicho plazo, se debe proceder a la supresión de las imágenes.

Si el responsable constata que se ha producido la grabación de un delito o infracción administrativa que deba ser puesta en conocimiento de la debida autoridad, y la denunciase, deberá conservar las imágenes a disposición de la citada autoridad.

4 ¿Existen limitaciones respecto a la ubicación y captación de los dispositivos de captación de imágenes?

4.1 ¿Puedo captar espacios públicos con mi sistema de seguridad?

Con carácter general, no se podrá captar vía pública a través de los sistemas de seguridad que instale el cliente en su empresa/negocio. Si bien, de manera excepcional podrá captarse vía pública en la medida en que sea imprescindible para preservar la seguridad de personas, bienes e instalaciones, siempre teniendo presentes los principios de proporcionalidad y necesidad.

Así, para que esta excepción resulte aplicable, deberá tenerse en consideración, por ejemplo, lo siguiente:

- No deberá existir una posibilidad de instalación alternativa.
- El cliente asegurará de que el impacto en los derechos de los viandantes sea el mínimo posible.

4.2 ¿Puedo captar propiedades privadas ajenas a la mía?

En ningún caso será admisible el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular en lo que se refiere a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

4.3 ¿Puedo captar imágenes de vestuarios, baños, salas de gimnasio…?

No. Este tipo de espacios están protegidos por el derecho a la intimidad cuya captación puede afectar a la propia imagen, la vida privada y a la protección de datos, por lo que no resulta posible la utilización de sistemas de videovigilancia en dichos entornos u otros equivalentes.

5 Supuestos especiales (instalaciones de las que pueden surgir otras limitaciones o prohibiciones).

5.1 Entornos escolares y menores

Los menores merecen una especial protección, por lo que el principio de proporcionalidad a la hora de instalar y utilizar sistemas de captación de imágenes debe aplicarse con un rigor extremo.

Por ello, en entornos como colegios, guarderías, centros lúdicos cuyo público objetivo sean los menores y espacios similares, la instalación de videocámaras sólo será legítima cuando exista una necesidad ineludible, cuando la medida sea la más adecuada y siempre que no exista una medida alternativa menos invasiva de los derechos del menor.

La instalación y uso de sistemas de captación de imágenes en entornos escolares o con menores debe ser proporcional al fin perseguido y que, en todo caso, debe ser legítimo.

Por ello, se tendrá en cuenta:

- La zona objeto de videovigilancia será la mínima imprescindible abarcando espacios públicos como accesos o pasillos.
- Salvo en circunstancias excepcionales, no resulta admisible la captación de imágenes con fines de control de asistencia escolar.
- El uso de videocámaras con fines de seguridad en espacios de juego, aulas y otros ámbitos en los que se desarrolla la personalidad de los menores sólo podrán ser objeto de grabación en presencia de circunstancias excepcionales, justificadas por la presencia de un riesgo objetivo y previsible para la seguridad de los menores.

5.2 Uso de sistemas de videovigilancia para control empresarial

El Estatuto de los Trabajadores faculta al empresario para adoptar las medidas que estime oportunas con el fin de vigilar y controlar el desarrollo de las obligaciones laborales de sus empleados, siempre teniendo en cuenta su dignidad humana, y la capacidad real de los trabajadores disminuidos, en su caso.

Si bien esta finalidad además de las obligaciones recogidas en el punto 3, deberá tener en cuenta otras cautelas como:

- Informar personalmente a los trabajadores y a la representación sindical, por cualquier medio que garantice la recepción de la información.
- No se deberán grabar conversaciones privadas de los empleados.
- Al realizar la declaración del fichero, deberá tenerse en cuenta la finalidad de control laboral, respecto de las imágenes obtenidas.

Estas prácticas, no obstante, se encuentran sometidas a la normativa de protección de datos de carácter personal, y deben cumplir con requisitos específicos. Puede consultarlos en la web de la Agencia.

Puede encontrar más información en la web de la Agencia.

5.3 Comunidades de propietarios

Para instalar y utilizar sistemas de videovigilancia en las zonas comunes de su Comunidad de Propietarios, además de las **obligaciones generales** establecidas, también deben tener en cuenta una serie de pautas. Algunas de ellas son:

- Será necesario autorización previa de la Junta de Propietarios que deberá constar en las actas correspondientes.
- Las cámaras solo podrán captar imágenes de las zonas comunes de la Comunidad. No se podrán captar imágenes de la vía pública ni espacios privados colindantes o cualquier otro espacio ajeno.
- El acceso a las imágenes estará restringido a las personas designadas por la Comunidad, y en ningún caso estarán accesibles a los vecinos mediante canal de televisión comunitario. Así mismo, el sistema de grabación se ubicará en un lugar vigilado o de acceso restringido.

Puede encontrar más información en la web de la Agencia.

5.4 Uso de sistemas de videovigilancia en mi plaza de garaje

La instalación y uso de sistemas de videovigilancia en su plaza de garaje, cuando ésta forma parte de un espacio compartido con el resto de propietarios, o con acceso a terceros, hace necesaria la aplicación de la legislación vigente en cuanto a protección de datos. Así, además de cumplir con las obligaciones generales, debe tener en cuenta una serie de pautas. Algunas de ellas son:

- Será necesario autorización previa de todos los propietarios (incluyendo terceros) debidamente formalizado.
- Las imágenes captadas por las cámaras se limitarán únicamente a su plaza de aparcamiento, y la franja mínima de espacios comunes que no se pueda evitar para la vigilancia de dicha plaza. En ningún caso se captarán imágenes de plazas de aparcamientos ajenas, vías públicas, terrenos colindantes o cualquier espacio ajeno.
- El acceso a las imágenes será exclusivamente del responsable del sistema, y en ningún caso serán accesibles a otras personas. Igualmente, el sistema de grabación se ubicará en un lugar vigilado o de acceso restringido.

Puede encontrar más información en la web de la Agencia.

Derechos ARCO

(Información relacionada con el punto 3.1.)

La normativa de protección de datos regula los siguientes derechos:

Derecho de acceso

El derecho de acceso permite al ciudadano conocer y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento.

Aplicado a la videovigilancia: el ejercicio del **derecho de acceso** reviste características singulares:

- Requiere aportar como documentación complementaria el aportar 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.

Ej. "Su imagen fue registrada en nuestros sistemas el día ___ del mes del año entre las _ horas y las _ horas. En concreto el sistema registra su acceso y salida del edificio.

Si se ejerciese el derecho de acceso ante el responsable de un sistema que únicamente reproduzca imágenes sin registrarlas deberá responderse en todo caso indicando la ausencia de imágenes grabadas.

Derecho de rectificación

Este derecho se caracteriza porque permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

Aplicado a la videovigilancia: no resulta posible el ejercicio del derecho de rectificación ya que por la naturaleza de los datos -imágenes tomadas de la realidad-, se trataría del ejercicio de un derecho de contenido imposible.

Derecho de cancelación

El derecho de cancelación permite que se supriman los datos que resulten ser inadecuados o excesivos sin perjuicio del deber de bloqueo recogido en la LOPD.

Aplicado a la videovigilancia: el derecho de cancelación solicitado por el afectado se rige por lo previsto en la LOPD sin especialidad alguna.

Derechos de oposición y limitación de tratamiento

Los derechos de oposición y limitación de tratamiento regulan el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo.

Aplicado a la videovigilancia: Si se interpretan como la imposibilidad de tomar imágenes de un sujeto concreto en el marco de instalaciones de videovigilancia vinculadas a fines de seguridad privada no resultaría tampoco posible su satisfacción en la medida en la que prevalecería la protección de la seguridad.