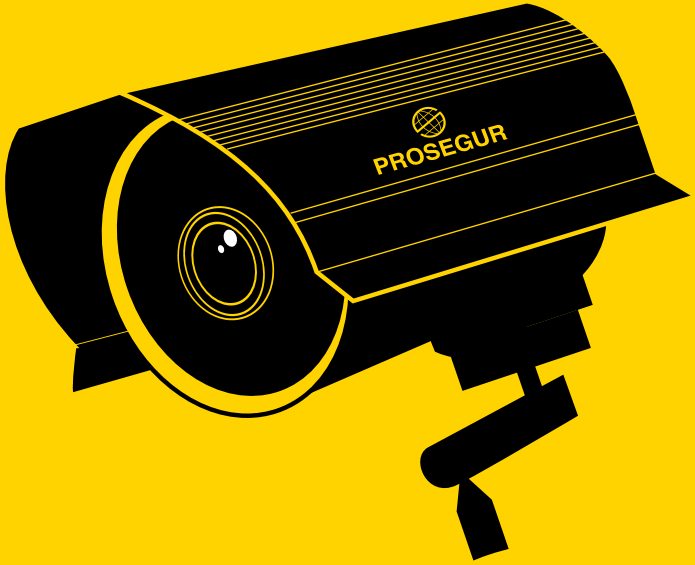

GUÍA DE ACTUACIÓN EN MATERIA DE PROTECCIÓN DE DATOS DE PROSEGUR EN SISTEMAS DE CAPTACIÓN DE IMÁGENES

PROSEGUR

ÍNDICE

1

INTRODUCCIÓN

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 Ley Orgánica 15/1999, de 13 de diciembre de protección de los datos de carácter personal (LOPD).

Esta Guía tratará de ofrecer indicaciones y criterios prácticos que permitan el adecuado cumplimiento de la legislación vigente en todos los casos.

2

CUÁNDO DEBEN APLICARSE LAS NORMAS SOBRE PROTECCIÓN DE DATOS A LOS TRATAMIENTOS DE IMÁGENES

El concepto de dato personal incluye las imágenes cuando se refieran a personas identificadas o identificables. Por ello, los principios vigentes en materia de protección de datos personales deben aplicarse al uso de cámaras, videocámaras y a cualquier medio técnico análogo, que capte y/o registre imágenes, ya sea con fines de vigilancia u otros en los supuestos en que:

a. Exista grabación, captación, transmisión, conservación, o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real o un tratamiento que resulte de los datos personales relacionados con aquellas.

b. Tales actividades se refieran a datos de personas identificadas o identificables. Para que se pueda utilizar un sistema de esta naturaleza no basta con que éste reúna los requisitos técnicos que lo permitan funcionar. Debe existir legitimación para ello. Esto ocurrirá cuando:

- Se cuente con el consentimiento del titular de los datos personales.
- Una norma con rango de Ley exima del consentimiento, como en los casos previstos por la Ley de Seguridad Privada o en el del artículo 20 del Estatuto de los Trabajadores.
- Se dé alguna de las circunstancias previstas por el artículo 6.2 LOPD u 11.2 LOPD que resulten de aplicación a este tipo de medios.

Además, si la legislación vigente impone algún requisito adicional éste deberá cumplirse.

3

CÓMO DEBEN TRATARSE Y CAPTARSE LAS IMÁGENES

El uso de las instalaciones de cámaras y videocámaras debe seguir ciertas reglas que rigen todo el proceso desde su captación, almacenamiento, reproducción hasta su cancelación. El responsable deberá tener en cuenta los siguientes principios:

- Debe existir una relación de proporcionalidad entre la finalidad perseguida y el modo en el que se traten los datos.

- Debe informarse sobre la captación y/o grabación de las imágenes.

- El uso de instalaciones de cámaras o videocámaras sólo es admisible cuando no exista un medio menos invasivo.

- Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos.

En cualquier caso el uso de sistemas de videovigilancia deberá ser respetuoso con los derechos de las personas y el resto del Ordenamiento jurídico.

- Ej. No sería admisible la captación de imágenes en espacios protegidos por el derecho a la intimidad como los interiores de viviendas cercanas, en baños o vestuarios o en espacios físicos ajenos al específicamente protegido por la instalación.

Las imágenes se conservarán por el tiempo imprescindible para la satisfacción de la finalidad para la que se recabaron.

- Ej. Como más adelante se señala en esta Guía la Instrucción 1/2006 sobre conservación de las imágenes con fines de vigilancia fija un plazo máximo de un mes.

4

CAPTACIÓN Y TRATAMIENTO DE IMÁGENES CON FINES DE SEGURIDAD

En este ámbito deben respetarse y aplicarse los principios contenidos en la legislación vigente y en particular la LOPD, el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (RDLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, y la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

Este cumplimiento se proyectará sobre distintos aspectos.

5

OBLIGACIONES

I. INSCRIPCIÓN DE FICHEROS

La utilización de sistemas de vigilancia mediante videocámaras puede dar lugar a la creación de ficheros. El RDLOPD precisa en qué casos existirá un fichero:

Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- Ej. Si se utiliza un sistema conectado a un ordenador que almacena las imágenes en un disco duro, o en cualquier otro soporte informático, y permite localizarlas atendiendo a criterios como el día y/u hora de grabación, el cruce de imágenes, el lugar físico registrado etc.

Si el sistema de videovigilancia genera un fichero el responsable deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma. Esto ocurrirá siempre que exista algún tipo de grabación.

La inscripción puede realizarse en el Registro de la Agencia Española de Protección de Datos mediante un modelo predefinido a través del sistema de Notificaciones Telemáticas-NOTA.

https://www.agpd.es/portalweb/canalresponsable/index-ides-idphp.php

Se adjunta un documento como **Anexo I** con los pasos a seguir para dar de alta el fichero a través de este procedimiento.

Hay sistemas que no registran imágenes y por ello la Instrucción 1/2006 señala que no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

- Ej. Circuitos cerrados de televisión controlados mediante visualización en pantalla.

Por tanto, no resulta necesario inscribirlos. Sin embargo, esto no exime del cumplimiento del resto de deberes establecido por la LOPD y la Instrucción 1/2006 que se detallan en esta Guía.

II. DEBER DE INFORMAR

La información en la recogida de los datos es un elemento esencial del derecho a la protección de datos y por tanto su cumplimiento resulta ineludible. Sin embargo las especiales características que se dan en la videovigilancia comportan el diseño de procedimientos específicos para informar a las personas cuyas imágenes se capten.

La Instrucción 1/2006 incorpora un distintivo informativo cuyo uso y exhibición es obligatoria. 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.

Se adjunta modelo como **Anexo II**.

Además el responsable del fichero dispondrá de un impreso con toda la información a la que se refiere el artículo 5 LOPD. Por tanto el impreso deberá informar al menos sobre:

a. 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.

b. La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

c. La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

El impreso deberá estar disponible existiendo cuando menos la posibilidad de imprimirlo a petición del afectado.

Se adjunta modelo como **Anexo III.**

III. CONTRATO DE ACCESO A LOS DATOS POR CUENTA DE TERCEROS

La implementación de sistemas de videovigilancia puede dar lugar a distintos tipos de prestación. Una empresa externa puede prestar servicios consistentes en:

a. Instalación y/o mantenimiento técnico de los equipos y sistemas de videovigilancia sin acceso a las imágenes. En este caso la empresa de seguridad no posee la condición de encargado de tratamiento correspondiendo al responsable, que la contrató, la adaptación de la instalación a los requisitos normativos.

- Ej. La simple instalación técnica de las cámaras y los equipos de grabación por una empresa de seguridad que actúa como instalador autorizado contratado por una comunidad de propietarios limitándose a tareas puramente técnicas que no comporten acceso a las imágenes.

b. Instalación y/o mantenimiento de los equipos y sistemas de videovigilancia con utilización de los equipos o acceso a las imágenes. Únicamente en este segundo caso, la empresa de seguridad será considerada encargada del tratamiento y la obligatoriedad de cumplir con las obligaciones de lo dispuesto por el artículo 12 LOPD.

- Ej. Las empresas de seguridad que prestan servicios combinados de central de alarmas y videovigilancia de modo que cuando se activa la alarma se comprueban directamente las imágenes por el personal de la empresa de seguridad.

c. Con carácter general, La instalación de sistemas de videovigilancia que se conecten a una Central Receptora de Alarmas con fines de seguridad privada comporta necesariamente la contratación de los servicios de empresas de seguridad debidamente autorizadas por el Ministerio del Interior.

* Por ello, cuando se capten y/o registren imágenes con fines de seguridad privada y la empresa de seguridad contratada utilice las videocámaras y/o acceda a las imágenes por medio de su personal resulta ineludible la celebración de un contrato de acceso a los datos por cuenta de terceros.

- PROSEGUR firma con sus clientes este contrato.

IV. DOCUMENTO DE SEGURIDAD

El Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la Ley Orgánica 15/1999 de Protección de Datos, establece en su artículo 88 la obligación del que el Responsable del fichero tienen de elaborar un Documento de Seguridad.

Es un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación para todos los responsables de ficheros con independencia del nivel de seguridad que sea necesario aplicar.

Los apartados mínimos que debe incluir el documento de seguridad son los siguientes:

a. Ámbito de aplicación.

b. Especificación detallada de los recursos protegidos.

c. Medidas, normas, procedimientos, reglas y estándares de seguridad.

d. Funciones y obligaciones del personal.

e. Estructura y descripción de los ficheros y sistemas de información.

f. Procedimiento de notificación, gestión y respuesta ante incidencias.

g. Procedimiento de copias de respaldo y recuperación de datos.

h. Medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

6

MEDIDAS DE SEGURIDAD

El responsable de la instalación deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de las imágenes y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Con carácter general los ficheros de videovigilancia suelen tener un nivel básico. No obstante el responsable del fichero debe tener en cuenta que deberá evaluar el nivel de seguridad teniendo en cuenta lo dispuesto por el artículo 81 del Reglamento en función del contenido y finalidad del fichero.

El responsable deberá informar a las personas con acceso a los datos sobre sus obligaciones de seguridad y su deber de secreto en los términos del artículo 8 de la Instrucción 1/2006.

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas. El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior.

7

CANCELACIÓN DE OFICIO DE LAS IMÁGENES

La Instrucción 1/2006 establece en su artículo 6 un plazo de cancelación máximo de un mes desde su captación.

Por tanto una vez transcurrido dicho plazo las imágenes deberán ser canceladas, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

En aquellos casos en los que el responsable constatase la grabación de un delito o infracción administrativa que deba ser puesta en conocimiento de una autoridad, y la denunciase, deberá conservar las imágenes a disposición de la citada autoridad.

8

DERECHOS DE LAS PERSONAS

El ejercicio de los derechos posee perfiles específicos en el ámbito de la videovigilancia.

a. 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.

b. Por otro lado, el ejercicio del derecho de oposición también plantea enormes dificultades. Si este se interpreta 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.

c. Por otra parte el ejercicio del derecho de acceso reviste características singulares:

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.

- 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.

d. La cancelación solicitada por el afectado se rige por lo previsto en la LOPD sin especialidad alguna.

* No debe olvidarse que conforme a las previsiones del RDLOPD en caso de denegación de un derecho deberá indicarse expresamente la posibilidad de reclamar su tutela ante el Director de la Agencia Española de Protección de Datos.

ANEXO I

CÓMO HACER LA NOTIFICACIÓN

La presentación de solicitudes de inscripción de ficheros podrá realizarse indistintamente en soporte papel, informático o telemático, aunque en cualquiera de los casos, su cumplimentación debe realizarse a través del formulario electrónico de Notificaciones Telemáticas a la AEPD **(NOTA)**.

El formulario electrónico no requiere una instalación previa en su equipo por lo que puede ser cumplimentado desde la página Web de la AEPD.

A continuación le indicamos cómo puede usted realizar la notificación de los ficheros.

Acceda a la Web de la Agencia: **www.aqpd.es**

Coloque el cursor encima de la opción:
RESPONS. FICHEROS

Seleccione la opción: **INSCRIPCIÓN DE FICHEROS**

Seleccione en la columna de la izquierda la opción: **Obtención del formulario NOTA**. El formulario NOTA es el formulario oficial para hacer la declaración de los ficheros en AEPD. La declaración del fichero se tiene que hacer obligatoriamente con este formulario. **AVISO: Es necesario que tenga en su ordenador un Adobe Reader versión 7.0.8 o superior**. En el final de la página encontrará el lugar dónde se encuentran las **Descargas disponibles:**

- Preguntas más frecuentes. Es un documento informativo que proporciona la AEPD.
- Guía rápida del formulario NOTA. Es un documento informativo que proporciona la AEPD.
- Manual del formulario electrónico de notificación de ficheros de Titularidad privada. Es un documento informativo que proporciona la AEPD.
- Formulario NOTA de Titularidad privada. Es el documento de notificación.
- Pulse en **Formulario NOTA de Titularidad privada:**

a. Preguntas iniciales del asistente:

1. **Tipo de solicitud de inscripción.** Deberá señalar la casilla de Alta.
2. **Modelo de declaración.** Deberá señalar en la casilla de Normal.
3. **Forma de presentación.** Deberá señalar en la casilla de Papel.

b. Cumplimentación de la notificación: Deberá cumplimentar los apartados del formulario que describan

el fichero que va a ser notificado.

El formulario NOTA consta de dos páginas de detalle y la correspondiente *Hoja de solicitud*. Deberá cumplimentar los siguientes apartados:

1. Responsable del fichero.
- *Denominación social del responsable del fichero:* Se deberá poner el nombre de la empresa o negocio.
- *Actividad:* Seleccione el tipo de actividad del responsable de fichero de la lista disponible en el formulario electrónico. Para visualizar los textos posicione el cursor en la tipificación correspondiente en el lugar de la fecha.
- *CIF/NIF:*
- *Domicilio Social:*
- *Localidad:*
- *Código Postal:*
- *Provincia:*
- *País:*
- *Teléfono:*
- *Fax:*
- *Correo electrónico:*

2. Derechos de oposición, acceso, rectificación y cancelación. Este apartado únicamente deberá cumplimentarlo en el caso de que la dirección dónde se prevee atender al ciudadano que desee ejercitar sus derechos de oposición, acceso, rectificación y cancelación sea diferente a la indicada en el apartado 1. *Responsable del fichero.*

PULSAR LA TECLA DE Validar.

3. Encargado de tratamiento. Este apartado únicamente habrá que cumplimentarse cuando un tercero realiza el tratamiento por cuenta del responsable. Deberá ser cumplimentado con los datos de quien trate los datos por cuenta del Responsable del tratamiento, por ejemplo con los datos de la empresa de seguridad que visiona sus imágenes en un salto de alarma.2. *Responsable del tratamiento*.

PULSAR LA TECLA DE Validar.

4. Identificación y finalidad del fichero:
- Denominación: Indique el nombre que identifique al fichero. “IMÁGENES DE SEGURIDAD”.
- Descripción detallada de la finalidad y usos previstos.
- Tipificación correspondiente a la finalidad y usos previstos: Seleccione en el lado de la izquierda VIDEOVIGILANCIA y luego pulse la > para que aparezca en el lado de la derecha.

PULSAR LA TECLA DE Validar.

5. Origen y procedencia de los datos:
- Origen: Se marcará en la casilla de El propio interesado o su representante legal.
- Colectivos o categorías de interesados: Seleccione en el lado izquierdo EMPLEADOS y pulse la > para que aparezca en el lado de la derecha. Marcar también la casilla de Otros colectivos.

PULSAR LA TECLA DE Validar.

6. Tipos de datos, estructura y organización del fichero:
- Datos de carácter identificativo: Marcar la casilla

de Imagen / voz.

- Otros datos tipificados: Seleccionar en el lado de la izquierda CARACTERÍSTICAS PERSONALES y luego pulse > para que aparezca en el lado de la derecha.
- Sistema de tratamiento: Seleccionar la casilla Automatizado.

PULSAR LA TECLA DE Validar.

7. Medidas de seguridad: Seleccionar la casilla Nivel básico.

PULSAR LA TECLA DE Validar.

8. Cesión o comunicación de datos: NO HAY QUE PONER NADA.

9. Transferencias internacionales: NO HAY QUE PONER NADA.

c. Cumplimentar y firmar la Hoja de solicitud:
Una vez que se ha comprobado que los distintos apartados han sido cumplimentados correctamente, deberá cumplimentar la Hoja de solicitud.

Deberá indicar los datos identificativos de la persona que firma la solicitud y el cargo o la condición del firmante de esta solicitud en relación con el responsable del fichero. Señale también la dirección completa a afectos de notificaciones.

Antes de realizar el envío de la notificación deberá leer y aceptar la información relativa a los deberes que conlleva la firma de la Hoja de solicitud.

d. Generar o enviar la notificación:
Una vez que haya cumplimentado la Hoja de solicitud, para obtener el modelo que puede ser presentado en AEPD, deberá pulsar el botón «Finalizar formulario» que se encuentra al final de la Hoja de solicitud. Se generará el código de barras bidimensional PDF 417 (nube de puntos), así como el correspondiente código de envío que establece la correspondencia entre el contenido que figura en cada una de las páginas que componen el modelo de notificación y la nube de puntos generada. Este sistema garantiza que la notificación ha sido cumplimentada de forma correcta y que se inscribirá en el RGPD de forma ágil, rápida y segura.

Se imprimirá la correspondiente notificación en la que figurará el código de barras bidimensional PDF 417 (nube de puntos). Una vez firmada la Hoja de solicitud por la persona que, con representación suficiente del responsable del fichero, formula la notificación, se presentará en ia AEPD. La dirección de la AEPD es: Agencia Española de Protección de Datos c. Jorge Juan, 6 28001 - Madrid.

ANEXO II

MODELO CLAÚSULA INFORMATIVA

Art. 3, apartado B. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

FICHERO PRIVADO

De conformidad con lo dispuesto en el art. 5.1 LO 15/1999, de 13 de diciembre, de Protección de Datos, se informa:

1. Que sus datos personales se incorporarán al fichero denominado "....." y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia.

2. Que el destinatario de sus datos personales es:

- **a.** La empresa de seguridad.
- **b.** El dueño del establecimiento.

3. Que puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante el responsable del fichero.

4. Que el responsable del fichero tratamiento es " (..... nombre o razón social.....)" o su representante "D./Da. ..... ubicado en C/ .....".

ANEXO III

PLACA INFORMATIVA

PROSEGUR

902 202 999
www.prosegur.es