Videovixilancia e Protección de datos

V. 3.0
Febreiro 2024

INTRODUCIÓN

Este documento ten por finalidade servir de base e axuda á hora do cumprimento dos deberes en materia de protección de datos intrínsecos ás entidades que conten con algún servizo ou sistema de videovixilancia proporcionado por **Sistemas de Seguridade A1** nas súas instalacións.

A normativa base de aplicación é:

- Regulamento UE 2016/679, do Parlamento Europeo e do Consello de 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos personais e á libre circulación destes datos (norma directamente aplicable).
- Lei Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Persoal e garantía dos dereitos dixitais.

Este manual foi elaborado como mecanismo de axuda, non pretende substituír as recomendacións que a súa entidade poida recibir ou recibise dos seus asesores en materia de protección de datos, nin ten un contido exhaustivo.

PREGUNTAS FRECUENTES

É necesario que a entidade actualice o seu rexistro de actividades de tratamento?

Si, as entidades que dispoñan dun sistema de videovixilancia deben crear a preceptiva actividade de tratamento "videovixilancia" para incluíla na súa RAT (Rexistro Actividades de Tratamento).

Que información debe incluir a actividade de tratamento "videovixilancia"?

A actividade de tratamento debe incluír a seguinte información:

- O n**ome e os datos de contacto do responsable** e, no seu caso, do corresponsable, do representante do responsable e, **de ser pertinente, o do delegado de protección de datos.**
- As **fins do tratamento.**
- Unha descrición das **categorías de interesados** e das **categorías de datos personais.**
- As **categorías de destinatarios** a quen se comunicou ou comunicarán os datos persoais, incluíndo os destinatarios en terceiros países ou organizacións internacionais.
- No seu caso, as **transferencias internacionais** de datos persoais a un terceiro país ou organización internacional, incluída a identificación de devandito terceiro país ou organización internacional, así como a documentación sobre garantías adecuadas para determinados casos.
- Os **prazos de conservación** das imaxes.
- E, cando sexa posible, unha descrición xeral das medidas técnicas e organizativas de seguridade que o responsable aplique para garantir a integridade e confidencialidade dos datos.

Que é unha avaliación de impacto en materia de protección de datos?

Trátase dunha ferramenta de carácter preventivo que debe realizar o responsable do tratamento para poder identificar, avaliar e xestionar os riscos aos que están expostas as súas actividades de tratamento co obxectivo de garantir os dereitos e liberdades das persoas físicas.

Cando sexa probable que un tipo de tratamento entrañe un alto risco para os dereitos e liberdades das persoas físicas, o responsable do tratamento realizará, unha avaliación de impacto das actividades de tratamento na protección de datos persoais.

A instalación e utilización do sistema de videovixilancia require habilitar medidas de seguridade e protocolos?

Si, xunto á creación da actividade de tratamento, en virtude do artigo 32 do RGPD a entidade debe aplicar medidas técnicas e organizativas apropiadas para garantir un nivel de seguridade adecuado ao risco, definíndoas en función do estado da técnica, os custos de aplicación, a natureza, o alcance, o contexto e as fins do tratamento.

Por risco deben entenderse todos aqueles activos que xeren probabilidade e gravidade para os dereitos e liberdades das persoas físicas no que respecta a os seus datos persoais.

No seu caso, froito da Análise de Riscos ou da Avaliación de Impacto implementaranse na entidade as medidas de seguridade que se establezan para minimizar os riscos.

A entidade responsable debe informar sobre a instalación e uso do sistema de videovixilancia?

Si, a entidade responsable está obrigada a informar da súa instalación e uso.

É importante ter en conta que, no suposto da videovixilancia, debemos distinguir entre a información para proporcionar a persoas empregadas, socios e, no seu caso, voluntarios (dependendo da entidade), da información para transmitir á cidadanía en xeral (visitantes que acceden ás instalacións ou clientes, por exemplo).

Dereito de información ao persoal laboral nos sistemas de videovixilancia:

Establécese a obrigación expresa de notificar a todo o persoal laboral a existencia e/o instalación dos sistemas de vixilancia mediante cámaras, así como a súa finalidade e os dereitos que lle amparan.

Recoméndase que dita información sexa entregada por escrito, quedándolle constancia fidedigna á entidade de que as persoas traballadoras recibiron dita información (sinatura da mesma nun documento informativo, acuse de recibo nun correo electrónico…).

Dereito de información en xeral:

A Axencia Española de Protección de Datos esixe a instalación de carteis informativos da existencia de cámaras de videovixilancia.

Por tanto, no caso da cidadanía en xeral atopámonos con dúas necesidades:

1ª.- O cartel informativo básico.

2ª.- A disposición en todo momento, baixo solicitude de calquera persoa interesada, a actividade de tratamento, onde se deben especificar a base lexitimadora, as finalidades, as posibles comunicacións de datos, as categorías de datos solicitados, o prazo de conservación e un resumo das medidas de seguridade aplicadas pola entidade para garantir a seguridade dos datos solicitados a través da videovixilancia, tal e como esixe o artigo 13 do RGPD.

Que información debe conter o cartel de aviso de cámaras de videovixilancia?

O contido mínimo do cartel será:

Responsable: os datos do responsable do tratamento (nome, dirección, identificación fiscal…).

Dereitos de protección: débese indicar como poden exercer as persoas os seus dereitos de protección de datos (como acceder, rectificar, cancelar, limitar o tratamento…).

Delegado de Protección de Datos: no seu caso, datos de contacto do DPD.

Información Adicional: facilitar a remisión ás persoas interesadas a un correo electrónico, departamento ou dirección na que poida solicitar toda a información relativa á actividade de tratamento.

A propia Axencia dispón a modo de exemplo dun modelo descargable do devandito cartel na seguinte ligazón:

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

Onde se debe colocar o cartel informativo? É necesario colocalo debaixo de cada cámara?

O cartel débese exhibir en lugar visible e, como mínimo, nos accesos ás zonas vixiadas, xa sexan interiores ou exteriores. No caso de que o espazo videovixiado dispoña de varios accesos, deberá dispoñerse de devandito distintivo de zona videovixiada en cada un deles.

O Gabinete Xurídico da Axencia Española de Protección de Datos pronunciouse respecto da localización do cartel informativo, explicitando que "*non é necesario que se coloque debaixo da/s cámara/s, senón que será suficiente colocar o distintivo informativo en lugar suficientemente visible, tanto en espazos abertos como pechados. Por tanto, resultaría aconsellable que se tratándose dun edificio sometido a videovixilancia, na entrada do mesmo, se situase o cartel informativo*".

Que dereitos poden exercer as persoas en relación co sistema de videovixilancia?

Aínda que os artigos 15 a 22 do RXPD regulan a totalidade dos dereitos que os interesados poden exercitar (acceso, rectificación, supresión, limitación do tratamento, portabilidade, oposición e oposición a decisións individuais automatizadas), o exercicio destes dereitos debe ser matizado no ámbito da videovixilancia.

A Axencia Española de Protección de Datos pronunciouse respecto diso:

En primeiro lugar, non resulta posible o exercicio do dereito de rectificación, xa que pola natureza dos datos (imaxes tomadas da realidade que reflicten un feito obxectivo) trataríase do exercicio dun dereito de contido imposible.

En segundo lugar, tampouco sería aplicable o dereito de portabilidade, xa que, aínda que se trata dun tratamento automatizado, a lexitimación non se basea nin no consentimento nin na execución dun contrato.

En terceiro lugar, non se aplicaría parte do contido do dereito á limitación do tratamento, no seu aspecto de "cancelación cautelar", que está vinculada ao exercicio dos dereitos de rectificación e oposición.

Por outra banda, si serían aplicables os seguintes dereitos:

- O **dereito de acceso**, aínda que este reviste características singulares, a que require achegar como documentación complementaria unha imaxe actualizada que permita ao responsable verificar e contrastar a presenza do afectado nos seus rexistros. Resulta practicamente imposible acceder a imaxes sen que poida verse comprometida a imaxe dun terceiro. Por iso, pode facilitarse o acceso mediante escrito certificado no que, coa maior precisión posible, e sen afectar a dereitos de terceiros, se especifiquen os datos que foron obxecto de tratamento.
- O **dereito de supresión**, con independencia do prazo máximo dun mes de supresión das imaxes.
- O **dereito á limitación do tratamento**, que se aplicaría na súa outra vertente, é dicir, solicítese ao responsable que se conserven as imaxes cando:
    - O tratamento de datos sexa ilícito e o interesado opóñase á supresión dos seus datos e solicite no seu lugar a limitación do seu uso.
    - O responsable xa non necesite os datos para as fins do tratamento, pero o interesado se os necesite para a formulación, exercicio ou defensa de reclamacións.

Que é un Encargado de Tratamento?

O encargado do tratamento é aquela entidade que realiza parte do tratamento dos datos baixo as instrucións e contrato do responsable de seguridade. Neste suposto, Sistemas de Seguridade A1, SL, é encargado do tratamento do sistema de videovixilancia instalado na súa organización.

O Considerando 81 do RXPD establece que o encargado do tratamento debe ofrecer suficientes garantías no referente a coñecementos especializados, fiabilidade e recursos, con vistas á aplicación de medidas técnicas e organizativas que cumpran os requisitos do RXPD, incluída a seguridade do tratamento.

Sistemas de Seguridade A1, SL garante que cumpre escrupulosamente coa normativa imposta polo Regulamento Europeo de Protección de Datos, cumprindo co establecido no Considerando 81 antes mencionado.

Así mesmo, o artigo 28 do RXPD esixe que o tratamento dos datos por parte do Encargado do Tratamento se rexa por un contrato que vincule ao encargado respecto do responsable, establecendo o contido mínimo do mesmo.

No devandito contrato, elaborado polo responsable do tratamento, impoñerá as instrucións, obrigacións con respecto ao tratamento dos datos a Sistemas de Seguridade A1, SL, así como os permisos do tratamento que concede á nosa entidade.

Sistemas de Seguridade A1, SL ofrécese á firma de canto contrato ou anexo precise para o cumprimento da súa obrigación, así como ao pleno sometemento do mesmo.

A entidade responsable do sistema de videovixilancia pode facilitar datos a terceiros?

A entidade está lexitimada para comunicar as imaxes captadas sen consentimento aos xuíces e tribunais así como ás Forzas e Corpos de Seguridade.

A base de lexitimación para os xuíces e tribunais está recollida na Lei Orgánica 6/1985, do 1 de xullo, do Poder Xudicial, e ás Forzas e Corpos de seguridade, polo antigo artigo 22 da LOPD.

A petición das gravacións por parte das Forzas e Corpos de Seguridade debe ser proporcional á finalidade do requirimento realizado, sen que se produza unha comunicación indiscriminada. A este respecto o artigo 22.2 da LOPD establece que "*a recollida e tratamento para fins policiais de datos de carácter persoal polas Forzas e Corpos de Seguridade sen consentimento das persoas afectadas están limitados a aqueles supostos e categorías de datos que resulten necesarios para a prevención dun* ***perigo real*** *para a seguridade pública ou para a represión de infraccións penais…*".

A Axencia Española de Protección de Datos en reiterados informes veu a interpretar este artigo (informe 16 xullo 1999, 213/2004, 0297/2005, 0145/2007, entre outros), considerando que o tratamento de datos por parte das Forzas e Corpos de Seguridade será posible a condición de que se cumpran os seguintes requisitos:

- Que quede debidamente acreditado que a obtención dos datos resulta necesaria para a prevención dun perigo real e grave para a seguridade pública ou para a represión de infraccións penais e que, tratándose de datos especialmente protexidos, sexan absolutamente necesarios para as fins dunha investigación concreta.
- Que se trate dunha petición concreta e específica, ao non ser compatible co sinalado anteriormente o exercicio de solicitudes masivas de datos.
- Que a petición se efectúe coa debida motivación, que acredite a súa relación cos supostos que se expuxeron.
- Que, en cumprimento do artigo 22.4 da LOPD, os datos sexan cancelados cando non sexan necesarios para as investigacións que motivaron o seu almacenamento.

CONCLUSIÓN: só se pode ceder cando a solicitude, que segundo sentenza do TC 14/2003, do 30 de xaneiro, debe conter xustificación razoada na recollida e tratamento de datos de carácter persoal para fins policiais, refírese a un caso concreto.

En canto á solicitude das imaxes por parte de particulares, para coñecer a identidade dun terceiro, para os efectos de poder exercitar determinadas accións xudiciais e/o contractuais, para poder facerse efectiva debe reunir os seguintes requisitos:

- Lexitimación: o interese lexítimo invocado polo particular debe referirse ao exercicio do dereito fundamental á tutela xudicial efectiva, na medida que as imaxes se utilizarán para a obtención de probas para formular unha posterior denuncia por delito, ou reclamación por responsabilidade contractual, ou extracontractual a unha compañía de seguros

- Finalidade compatible: esta comunicación de datos non persegue unha finalidade diferente coa que se recolleron os datos, pois entra dentro do termo amplo de "seguridade".
- Minimización de datos: a cesión debe limitarse ao mínimo necesario para a finalidade pretendida, na medida que o solicitante poida determinar exclusivamente o relacionado co incidente concreto a que se refire a súa petición.

En todo caso, como responsable do tratamento que é a súa entidade, de conformidade coa Lei de Axuizamento Criminal, debe ser a organización quen dea traslado do presunto delito ás autoridades competentes.

A este respecto pronunciouse en numerosas ocasións a Axencia Española de Protección de Datos, chegando a recomendar nalgúns supostos que sexa directamente a organización a que dea traslado das imaxes ás autoridades sen comunicar os datos ao presunto responsable cando a causa dos danos fose delituosa.

Recomendamos a lectura da resposta a unha consulta exposta a esta respecto polo Gabinete xurídico da Axencia Española de Protección de Datos: https://www.aepd.es/media/informes/informe-juridico-rgpd-interes-legitimo.pdf

¿A entidade ten a obrigación de designar que persoas teñen acceso ás imaxes?

A entidade responsable do tratamento deberá designar as persoas concretas que van ter acceso ás imaxes que constarán como persoas usuarias autorizadas no documento da Análise de Riscos. Previamente deberán ser informadas e aceptar por escrito as súas respectivas responsabilidades.

Existe un prazo máximo de conservación das imaxes?

A normativa prevé un tempo máximo no que poden gardarse as imaxes dun sistema de videovixilancia en 30 días; por tanto, non se exclúen períodos de conservación inferiores ao máximo.

Aínda que existen causas especiais que poden prolongar ese período. Por exemplo, se hai unha investigación policial ou xudicial en curso, o tempo de almacenamento estenderase á duración desta.

RESUMO OBRIGACIÓNS RELACIONADAS COAS CÁMARAS

As obrigacións mínimas que debe de cumprir unha entidade ao contar cun sistema de videovixilancia serán as seguintes:

- Colocación en lugares visibles das instalacións de placas de aviso para informar ás persoas usuarias da existencia dun sistema de videovixilancia. O cartel indicará de forma clara a identidade do responsable do tratamento, ante quen e onde dirixirse para exercer os dereitos que prevé a normativa de protección de datos e onde obter máis información sobre o tratamento dos datos persoais.

- Notificar por escrito a todo o persoal da entidade de que os espazos de traballo teñen instalado un sistema de videovixilancia.

- Dispoñer de documento informativo sobre o uso de videocámaras ao dispor das persoas usuarias que o soliciten.

- As imaxes captadas polas cámaras limitaranse ao espazo de que se trate, salvo que sexa imprescindible para a finalidade perseguida. Non poderán captarse imaxes da vía pública a excepción dunha franxa mínima dos accesos ao establecemento. Tampouco poderán captarse imaxes de terreos e vivendas lindeiros ou de calquera outro espazo alleo. Se se utilizan cámaras orientables e/ou con zoom, será necesaria a instalación de máscaras de privacidade para evitar captar imaxes da vía pública, terreos e vivendas de terceiros.

- As cámaras só captarán imaxes dos espazos indispensables para esta finalidade. En ningún caso se situarán en zonas de vestiarios, baños e espazosde descando das persoas traballadoras.

- O sistema de gravación situarase nun lugar vixiado ou de acceso restrinxido. Ás imaxes gravadas accederán só as persoas autorizadas que deberán introducir un código de usuario e un contrasinal persoal e intransferible.

- As imaxes serán conservadas durante un prazo máximo dun mes dende a súa captación, transcorrido o cal se procederá á súa total destrución, salvo as excepcións previstas pola normativa.