Protección de datos: Principios generales

CPR 2019\208

Planteamiento

¿Qué se entiende por “datos relativos a la salud”?

¿Tienen los datos relativos a la salud de una persona especial protección?

¿En qué base legitimadora puede basarse mi organización para tratar datos relativos a la salud de una persona?

Las Mutuas de Accidentes ¿son responsables o encargadas de tratamiento?

¿Cómo debo informar a mis pacientes del tratamiento de sus datos?

Tengo cámaras de videovigilancia en mi organización, ¿debo de avisar de su existencia? ¿cómo? ¿puedo usar las imágenes para controlar el desempeño laboral de mis trabajadores?

Respuestas

1.

No existiendo dudas sobre el carácter personal de los datos relativos a la salud, la LOPD no contenía una definición de dicho concepto (y no será porque no tuviera definiciones en su articulado). Esta carencia se corrigió con el Reglamento que desarrollaba la LOPD que contenía una definición de los datos de carácter personal relacionados con la salud en su art. 5.1. g) a cuyo tenor

Datos de carácter personal relacionados con la salud : las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

Por su parte, el art. 3. j) de la Ley 14/2007, de Investigación Biomédica definía el dato genético como la “ información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científicos”.

De igual modo, el RGPD también ha recogido un concepto sobre este tipo de datos y los datos genéticos en los considerandos 34 y 35:

Considerando 34 : Debe entenderse por datos genéticos los datos personales

relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

Considerando 35 : Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo 9; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

Tener claro cuando estamos tratando un dato relativo a la salud de una persona física o un dato genético es muy importante, pues como veremos en esta guía, la normativa de protección de datos otorga una especial protección a este tipo de datos, lo que debe ser tenido en cuenta por las organizaciones que realicen un tratamiento de los mismos, tanto a efectos de obligaciones que deben asumir, como de eventuales sanciones derivadas de la comisión de infracciones por un tratamiento indebido de este tipo de datos que ahora pueden ser sancionadas con multas administrativas de hasta 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

2.

En nuestra tradición jurídica los datos relativos a la salud han gozado de una especial protección, y como no podía ser de otro modo, el RGPD continua con esta tradición de sobreprotección hasta el punto de prohibir su tratamiento como regla general en su art. 9.1, no permitiéndose su tratamiento si no concurre alguna de las excepciones previstas en su apartado 2.

Esta especial protección también va a conllevar que los responsables y encargados de tratamiento que traten datos de salud asuman obligaciones tales como:

La llevanza de un registro de actividades de tratamiento (art. 30 RGPD)

La realización de Evaluaciones de Impacto cuando exista un tratamiento a gran escala de datos de salud (art. 35 RGPD).

La designación de un Delegado de Protección de Datos cuando la actividad del responsable consista en el tratamiento a gran escala de datos de salud (vg. el tratamiento que lleva a cabo un hospital)

La realización de un Análisis de Riesgos para determinar las medidas técnicas y organizativas a implementar para garantizar los derechos y libertades de los interesados.

Esta especial protección también aparece reflejada en el régimen sancionador instaurado por el RGPD donde se sanciona con multas administrativas de hasta 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, cuando se traten datos de salud sin respetar los principios tales como el de licitud que implica que el tratamiento de un dato relativo a la salud se encuentre amparo en una base legitimadora contemplada en el art. 9.2 RGPD.

3.

El nuevo marco normativo en materia de protección de datos ha abierto el abanico de posibilidades más allá del consentimiento del interesado para tratar datos de carácter personal.

Al ser los datos de salud datos especialmente protegidos, su tratamiento debe ampararse en una de estas bases legitimadoras del tratamiento:

El consentimiento explícito del interesado : no valdrá un mero consentimiento tácito, y aunque la LAP autoriza en su art. 8[1] el consentimiento verbal, considero que los problemas de prueba que conlleva este tipo de forma de recabar el consentimiento a la hora de demostrar la responsabilidad proactiva de las organizaciones, aconseja a que se opte como regla general por un consentimiento escrito u otras formas que faciliten la prueba como grabaciones de audio o vídeo . Consentimiento escrito que en todo caso será necesario en los supuestos contemplados en el citado art. 8.2 LAP.

El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice una norma legal estatal o comunitaria, o un convenio colectivo: tendremos que entrar a valorar si una norma como el Estatuto de los Trabajadores, o la Ley de Prevención de Riesgos Laborales, nos autoriza a realizar este tipo de tratamiento, incluso podremos ampararnos en un convenio colectivo sectorial; la duda podría surgir respecto de la posibilidad de acudir a un acuerdo de empresa; en opinión de este autor, ello no sería posible, al estar ante datos especialmente protegidos donde la interpretación de la norma debe ser estricta sin que quepan extensiones

analógicas que lo que harían sería limitar el derecho fundamental a la protección de datos de los interesados.

El tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física , en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento: no debemos perder de visa que esta base legitimadora sólo entrará en juego cuando el interesado no pueda prestar su consentimiento libremente . Este supuesto se regula en el art. 9 LAP, donde se permite el consentimiento por representación:

Cuando el paciente no sea capaz de tomar decisiones, a criterio del médico responsable.

Cuando el paciente tenga la capacidad modificada judicialmente por sentencia.

Cuando el paciente menor de edad no pueda comprender el alcance de la intervención.

El tratamiento se refiera a datos personales que el interesado ha hecho manifiestamente públicos : aquí entrará en juego la publicación del interesado de sus datos en redes sociales, foros, blogs u otros servicios análogos.

El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial .

El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social , sobre la base de una norma legal estatal o comunitaria o en virtud de un contrato con un profesional sanitario, siempre y cuando dicho tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes: esta base jurídica será la que justifique el tratamiento clínico asistencial de un paciente por parte de un profesional o un centro sanitario, conteniéndose en la disposición adicional 17.ª de la LOPDGDD un listado con las normas de rango legal que legitiman este tratamiento. Por lo tanto, cuando un paciente viene a la consulta de un profesional sanitario por primera vez, no será necesario recabar su consentimiento, salvo para los tratamientos en los que se exige un consentimiento informado por escrito (intervención quirúrgica, procedimientos diagnósticos y terapéuticos, invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente) dado que estaremos legitimados al tratamiento de sus datos de salud por esta base jurídica legitimadora.

El tratamiento es necesario por razones de interés público en el ámbito de la salud pública , como la protección frente a amenazas transfronterizas graves para la

salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de una norma legal estatal o comunitaria, derechos y libertades del interesado, en particular el secreto profesional.

El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos : en este sentido, el apartado segundo de la disposición adicional 17.ª regula los criterios que rigen el tratamiento de datos en la investigación en salud.[2]

1 Artículo 8 LAP : Consentimiento informado 1. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4, haya valorado las opciones propias del caso. 2. El consentimiento será verbal por regla general. Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente. 3. El consentimiento escrito del paciente será necesario para cada una de las actuaciones especificadas en el punto anterior de este artículo, dejando a salvo la posibilidad de incorporar anejos y otros datos de carácter general, y tendrá información suficiente sobre el procedimiento de aplicación y sobre sus riesgos. 4. Todo paciente o usuario tiene derecho a ser advertido sobre la posibilidad de utilizar los procedimientos de pronóstico, diagnóstico y terapéuticos que se le apliquen en un proyecto docente o de investigación, que en ningún caso podrá comportar riesgo adicional para su salud. 5. El paciente puede revocar libremente por escrito su consentimiento en cualquier momento.

2 Disposición adicional decimoséptima LOPDGDD : Tratamientos de datos de salud 2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios: a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora. salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública. c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del 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 sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato. Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación. d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica. El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá: 1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación. 2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando: i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación. ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria. e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE)

2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando: 1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados. 2.º El ejercicio de tales derechos se refiera a los resultados de la investigación. 3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley. f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a: 1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos. 2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica. 3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados. 4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014 , si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679. g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial. En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679. h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Del estudio de este nuevo marco normativo, lo que nos tiene que quedar claro es que no siempre que se traten datos relativos a la salud, se requerirá como regla general el consentimiento del interesado, como establecía la LAP, en tanto en cuanto puedan existir normas de rango legal que legitimen dicho tratamiento, o puede concurrir una urgencia vital, existiendo, por tanto, otras bases jurídicas que legitiman el tratamiento de este tipo de datos , debiendo examinar el operador jurídico caso por caso la base concreta que legitima el tratamiento que se quiera realizar.

4.

Señala el art. 4 RGPD que «responsable del tratamiento» es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

El mismo art. 4 RGPD indica que es «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

Las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social son, según resulta del artículo 80 de la Ley General de la

Seguridad Social (en adelante LGSS), asociaciones debidamente autorizadas por el Ministerio de Trabajo y Asuntos Sociales, cuyo objeto principal es colaborar en la gestión de la Seguridad Social.

La LGSS regula la obligatoria afiliación de los Trabajadores por cuenta ajena, estableciendo la obligación de los empresarios de afiliación de sus trabajadores y establecer bien la protección de los mismos a través de una entidad gestora o de una Mutua de Accidentes de Trabajo y Enfermedades Profesionales.

Cuando el empresario opta por la protección de sus trabajadores a través de una Mutua, cede los datos de aquellos a ésta en virtud de una norma legal, no por un contrato, por lo que la Mutua estará actuando en concepto de Responsable del Tratamiento , y por lo tanto no será necesaria la firma del correspondiente contrato de encargado de tratamiento previsto en el art. 28 RGPD con las empresas que les cedan los datos de sus trabajadores.

Ambas, la empresa cedente de los datos y la mutua cesionaria de los mismos deberán asumir las obligaciones que impone la normativa de protección de datos a los Responsables del Tratamiento.

5.

En este punto debemos diferenciar el derecho a la información que tienen los pacientes a que se les informe sobre cualquier actuación en el ámbito de su salud, es decir, la información clínico-asistencial, que conforme al art. 4 LAP se le proporcionará cada vez que se lleve a cabo un nuevo acto médico verbalmente, dejando constancia en la historia clínica, y que comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias a efectos de que el paciente pueda ejercer su derecho de autodeterminación a través del consentimiento informado, de la información que debemos proporcionarle como titular de unos datos que le identifican como persona (datos identificativos como nombre, apellidos, documento de identidad, etc..), que se deberá proporcionar la primera vez que se recojan los datos el interesados pero que no deberá repetirse salvo que haya cambiado la finalidad del tratamiento de los datos, el responsable u otra circunstancia que el interesado deba conocer.

Uno de los principios del RGPD es el principio de transparencia, que implica que los datos serán tratados de forma transparente, el art. 13 RGPD regula la información que se debe facilitar a los interesados.

Se da la paradoja que la información que ahora se nos solicita que proporcionemos a los interesados es mayor que la que se nos venía pidiendo en el derogado art. 5 LOPD, y además el art. 12 RGPD nos pide que esta información la proporcionemos “en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado

por otros medios.”

¿Colmo solventamos este dilema? Pues la respuesta nos ha venido facilitada por las Autoridades de Control Españolas (la nacional, la vasca y la catalana) que abogan por que se realice la información a los interesados en dos capas informativas, al estilo de lo que se venía haciendo con la política de cookies. En este sentido las autoridades de control publicaron una guía para el cumplimiento del deber de informar accesible en su página web www.aepd.es.

La LOPDGDD ha dado carta de naturaleza legal a esta forma de informar en dos capas, y en su art. 11 señala que el responsable del tratamiento podrá dar cumplimiento a este deber facilitando una información básica que haga referencia a:

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

La finalidad del tratamiento.

La posibilidad de ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento

Indicar si se va a realizar elaboración de perfiles.

Posibilidad de oponerse a decisiones individuales automatizadas cuando produzcan efectos jurídicos o le afecten significativamente.

Cuando los datos no se obtengan del interesado:

Categorías de datos objeto de tratamiento

Fuente de procedencia de los datos

Ver formulario 1: PRIMERA CAPA INFORMATIVA

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS	
Responsable del tratamiento	Organización Sanitaria Ejemplo
Finalidad	Gestionar sus solicitudes de prestación sanitaria. Comunicarle por medios electrónicos sus citas. Gestión de su historia clínica. Trámites administrativos relacionados con la

	prestación del servicio sanitario y su facturación. Comunicar su número de habitación. Entrega a sus familiares de justificantes de su ingreso a efectos de obtener permisos retribuidos.
Derechos	Tienes derecho a acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puedes consultar toda la información adicional sobre nuestra política de protección de datos en nuestra web: https://www.organizacionejemplo.es/index.php/politicadeprivacidad/

Junto con esta información básica, se deberá indicar una dirección electrónica (por ejemplo, la página web de la organización) u otro medio (por ejemplo, una hoja en las oficinas visible para el público) que permita acceder a la segunda capa informativa que contendrá la siguiente información detallada del tratamiento de datos que realiza la organización:

INFORMACIÓN DETALLADA	
Responsable	• Datos de contacto del Responsable. • Identidad y datos de contacto del representante. • Datos de contacto del Delegado de Protección de Datos.
Finalidad	• Descripción ampliada de los fines del tratamiento.

	• Plazos o criterios de conservación de los datos. • Decisiones automatizadas, perfiles y lógica aplicada.
Legitimación	• Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo. • Obligación o no de facilitar datos y consecuencias de no hacerlo.
Destinatarios	• Destinatarios o categorías de destinatarios. • Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables.
Derechos	• Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento. • Derecho a retirar el consentimiento prestado. • Derecho a reclamar ante la Autoridad de Control.
Procedencia de los datos (cuando no precedan del interesado	• Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público. • Categorías de datos que se traten.

De esta manera se pretende evitar las largas cláusulas informativas que se estilaban con la LOPD que asusten a los interesados a la hora de afrontar su lectura

y comprensión, y eviten en definitiva lo que se pretende conseguir por el RGPD, la transparencia , que el interesado de un vistazo pueda conocer quién trata sus datos, para qué los trata y qué derechos tiene.

6.

La imagen de una persona en la medida que lo identifica constituye un dato de carácter personal y, por lo tanto, su tratamiento queda sujeto al cumplimiento de la normativa de protección de datos.

La LOPDGDD ha regulado el tratamiento de la videovigilancia para dos fines distintos, con fines de seguridad (art. 22) y con fines de control laboral (art. 89), veamos las especialidades de cada tratamiento.

FINES DE SEGURIDAD

Cuando el tratamiento de imágenes se realice con fines de seguridad debe valorarse la legitimación para utilizar estas imágenes y los principios de finalidad y minimización de datos, por ello, antes de instalar un sistema de videovigilancia debe tenerse presente lo siguiente:

Cuando la finalidad de la videovigilancia consiste en garantizar la seguridad de personas, bienes e instalaciones, es el interés público quien legítima dicho tratamiento.

Solo podrán captarse imágenes de la vía pública en la medida que resulten imprescindible. Como regla general, solo las Fuerzas y Cuerpos de Seguridad pueden captar imágenes de la vía pública.

Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo que hubieren de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones, en cuyo caso deben ser puestas a disposición de la autoridad competente en el plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

Tenemos el deber de informar de que estamos en una zona videovigilada, deber que se entenderá cumplido con la existencia de un dispositivo informativo en lugar suficientemente visible.

Ver formulario 2: Cartel informativo de videovigilancia

Tener a disposición de los afectados la segunda capa informativa con información detallada del tratamiento de datos que se realiza que deberá contener:

FINES DE CONTROL LABORAL

Se legitima el uso de videovigilancia con fines de control laboral al amparo de lo dispuesto en el art. 20.3 del Estatuto de los Trabajadores, si bien se debe tener presente lo siguiente:

El empleador debe de informar con carácter previo, de forma expresa, clara y

concisa, a los trabajadores o empleados públicos y, en su caso, a sus representantes, sobre esta medida. Nótese que la obligación es informar, no obtener su consentimiento, por lo que una comunicación por escrito (carta, correo electrónico, tablón de anuncios) sería suficiente para entender cumplido este requisito, si bien, no será suficiente la colocación del cartel informativo.

Si se capta la comisión de un acto ilícito por los trabajadores o empleados públicos, se entenderá cumplido el deber de informar con la colocación del cartel informativo. En este sentido debemos hacer referencia a una reciente sentencia dictada por el Juzgado de lo Social Tres de Pamplona, de fecha 18-02-2019, en el procedimiento de despido n.º 875/2018, en la que el Magistrado considera que no es suficiente la colocación del cartel informativo para que los trabajadores se den por informados de que las imágenes se pudieran utilizar para sancionarles o incluso despedirles, en tanto en cuanto considera que la LOPDGDD está limitando el derecho de información contenido en el art. 13 RGPD, siendo de preferente aplicación éste, en tanto estamos ante un Reglamento Europeo, dotado de eficacia directa y primacía frente a toda norma nacional que contradiga su contenido, conforme a la jurisprudencia emanada del Tribunal de Justicia de la Unión Europea (en adelante TJUE) que establece que en caso de contradicción entre la norma nacional y la comunitaria, la primera debe interpretarse de conformidad con la comunitaria, si ello fuera posible y, en caso contrario, dejar inaplicada la normativa nacional en favor de la aplicación de la comunitaria, todo ello siempre que la contradicción sea evidente, ya que si no lo es, la cuestión debe someterse, mediante cuestión prejudicial, al TJUE. Por todo ello el Juzgado de los social tres de Pamplona, no aplica lo dispuesto en el art. 89.1 segundo párrafo, y declara nula la prueba obtenida con la videovigilancia por vulnerar un derecho fundamental como es el de la protección de datos.

Las cámaras solo captarán imágenes de los espacios indispensables para el control laboral. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o empleados públicos, tales como vestuarios, aseos, comedores y análogos.