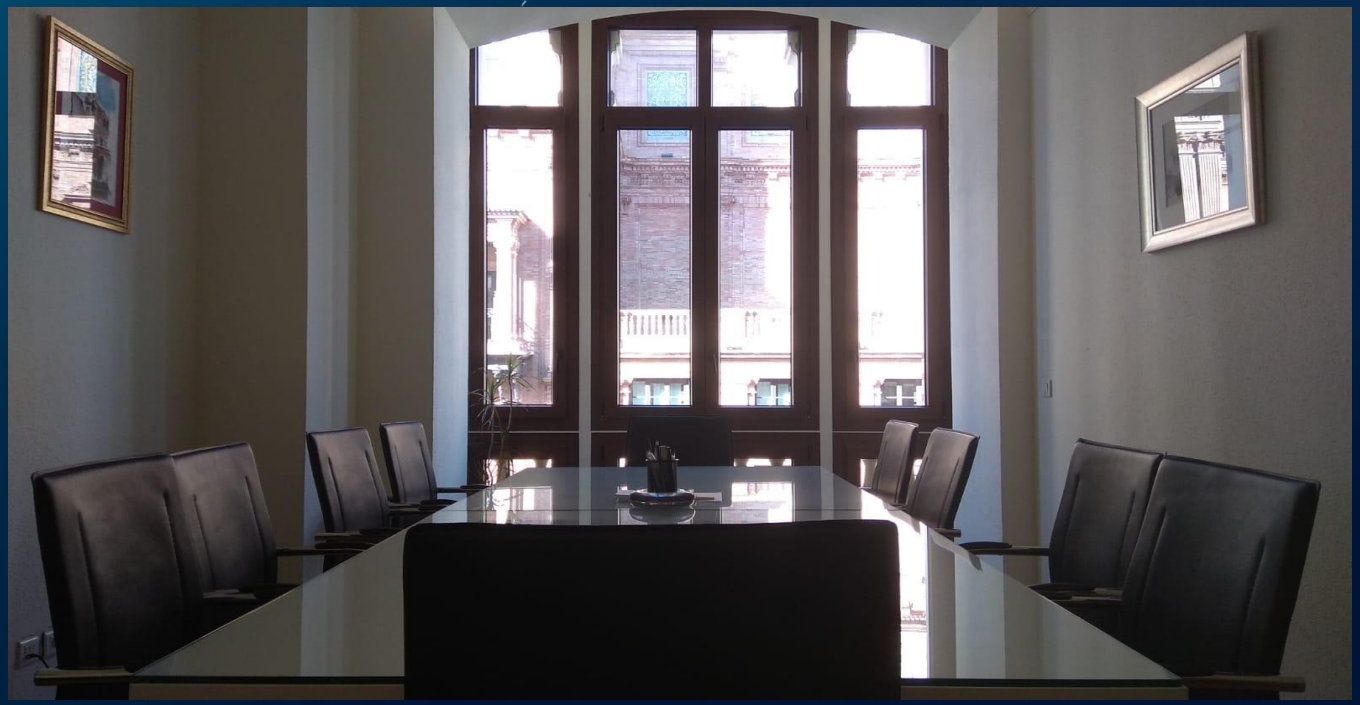
CREMADES & CALVO-SOTELO
ABOGADOS

www.cremadescalvosotelo.com



JORNADA PROTECCION DE DATOS
DIPUTACION DE BADAJOZ

1.CONCEPTOS BÁSICOS

DATO PERSONAL

"Toda información sobre una persona física identificada o identificable («el afectado»);
Persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, etc

1.CONCEPTOS BÁSICOS

DATO PERSONAL

Los datos personales se pueden agrupar por categorías en función del tipo de datos que tratemos:

- Datos económicos: cuenta corriente.
- Datos profesionales: profesión, sitios donde se ha trabajado.
- Datos de localización: calle, dirección, teléfono
- Datos de identificación: nombre, apellido, mote.

1.CONCEPTOS BÁSICOS

CATEGORIAS ESPECIALES. DATOS ESPECIALMENTE PROTEGIDOS

1.- Datos relativos a la salud (física o mental).

2.- Datos genéticos: datos sobre características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

3.- Datos biométricos": datos personales obtenidos a partir de un tratamiento técnico especifico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos

4.- Datos que revelen ideología, afiliación sindical, religión y creencias.

5.- Datos que hagan referencia al origen racial, o a la vida sexual.

6.-Datos se refieran a la comisión de infracciones penales o administrativas

Datos de menores.- Actualmente fijada en 14 años la edad para prestar consentimiento en el tratamiento de datos (articulo 7 LOPDGDD).

1. CONCEPTOS BÁSICOS

CATEGORIAS ESPECIALES. DATOS ESPECIALMENTE PROTEGIDOS

En relación con esto datos hay que adoptar medidas especiales, especiales cautelas, la normativa Prohibe a priori su tratamiento. Con excepciones:
- Consentimiento.
- Son tratados dentro del marco de actividades legitimas de asociaciones, fundaciones.
- Lo establezca el derecho de la Unión o del Estado , en interés público: ámbito de la legislación laboral, fines de seguridad, alerta sanitaria, prevención y control de la salud y control de epidemias, gestión de servicios de asistencia sanitaria, ejercicio de derecho de defensa de reclamaciones, fines estadísticos, históricos o de investigación.

1. CONCEPTOS BÁSICOS

TRATAMIENTO

Cualquier actividad en la que estén presentes datos de carácter personal constituirá un tratamiento de datos, ya se realice de manera manual o automatizada, total o parcialmente, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

1. CONCEPTOS BÁSICOS

RESPONSABLE

Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

En el ámbito de la Administración Local, el responsable del tratamiento, considerando la normativa de régimen local aplicable, recaerá en los municipios, diputaciones provinciales e islas.

- Diputaciones.- Tratamientos propios (recursos humanos, video vigilancia de sus instalaciones..) serán responsables.

- Diputaciones- Presten un servicio derivado a favor del ayuntamiento, serán encargados.

1. CONCEPTOS BÁSICOS

ENCARGADO

Persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos por cuenta del responsable del tratamiento.

CONTRATO DE ENCARGADO.

Las relaciones entre Responsable y Encargado deben regularse en un contrato o instrumento jurídico.

2. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Desaparecen los ficheros.

Registro es un inventario de tratamientos.

Ha de contener →

- Responsable
- categoría de datos tratados
- fines del tratamiento
- contacto del dpd
- categoría de afectados
- tiempo conservación
- cesión de datos o trasferencias internacionales
- plazos de supresión
- legitimación del tratamiento
- medidas de seguridad.

3. PRINCIPIOS QUE DEBEN CUMPLIR LAS ADMINISTRACIONES EN EL TRATAMIENTO DE DATOS

1.- Licitud, lealtad y transparencia.

a) Licitud = **Legitimación para tratarlos..-** Se exige tanto para tratar datos como para cederlos, que exista una base legitimadora de las 6 que a continuación se enumeran:

- Consentimiento (No tácito) (expreso, libre, informado).
- Ejecución de un contrato o medidas precontractuales.
- Proteger intereses vitales.
- Satisfacer intereses legítimos (de un 3º).
- Cumplimiento de una obligación legal.

Nueva ley de contratos, requiere publicación de los datos miembros de la mesa de contratación. Cuando la administración los publica está cumpliendo con una obligación legal. Igual la comunicación de datos a la agencia tributaria.

El Ayto utiliza datos del Padrón para fomentar la participación ciudadana en base a la obligación legal establecida en la LBRL, de facilitar información sobre las actividades que lleva a cabo y facilitar su participación en la vida local.

Facilitar a los concejales de la oposición el acceso a documentación.- Dentro del ejercicio de la actividad de control que estos realizan. LBRL, establece una obligación de facilitar cuantos datos, antecedentes o documentos resulten necesarios para dicha labor

3.PRINCIPIOS QUE DEBEN CUMPLIR LAS ADMINISTRACIONES EN EL TRATAMIENTO DE DATOS

- Publicaciones de sanciones en el BOE en cumplimiento de la Ley de procedimiento administrativo, que establece dicha notificación para el caso de paradero desconocido del interesado.
Fuera de los supuestos establecidos en la Leyes, necesidad de consentimiento. (Ej. Publicación licencias en web)

- Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

(Normas competenciales: Tratamientos en el marco de sus competencias: Ley de carreteras, ley de subvenciones, ley de medioambiente …)
Estos 2 últimos son los que se dan en la administración y ambos precedidos de una ley (Ley de bases locales, normativa de función pública, texto ref. haciendas locales).

B) Transparencia = Deber de Información.
Lenguaje claro y sencillo.
Información por capas.
1 capa: Nombre del responsable, finalidad, legitimación, si se van a ceder los datos a 3º, si se va a realizar transferencia internacional, ejercicio de derechos.
2 capa: contiene la información adicional relativa a la posibilidad, plazos de conservación o criterio para determinarlo, datos de contacto de dpd, fines del tratamiento ampliado, derecho a reclamar ante la autoridad de control.

3.PRINCIPIOS QUE DEBEN CUMPLIR LAS ADMINISTRACIONES EN EL TRATAMIENTO DE DATOS

2.- Limitación de la finalidad
Recogidos para fines determinados, expresos y legítimos.
No tratados para fines incompatibles.
No es incompatible: archivo, investigación, estadística.

3.- Minimización de datos
Datos estrictamente necesarios para los fines. Adecuados y pertinentes.

4.- Exactitud.
Exactos y actualizados.

3.PRINCIPIOS QUE DEBEN CUMPLIR LAS ADMINISTRACIONES EN EL TRATAMIENTO DE DATOS

5.- <u>Limitación del plazo de conservación.</u>

No más tiempo del necesario para la finalidad del tratamiento.

Ha de informarse sobre el plazo o sobre los criterios para determinarlos.

Ej: Videovigilancia, plazo de 1 mes.

Más tiempo con fines investigación, estadístico o haya un interés público, siempre con la adopción de medidas del reglamento.

3. PRINCIPIOS QUE DEBEN CUMPLIR LAS ADMINISTRACIONES EN EL TRATAMIENTO DE DATOS

6.- <u>Integridad y seguridad</u>

El tratamiento ha de garantizar la seguridad de los datos.

Protegerlos de: accesos ilícitos, perdida, destrucción, daño, aplicando las medidas técnicas y organizativas necesarias.

7.- <u>Responsabilidad proactiva</u>

Responsable del tratamiento, es responsable de cumplir estos principios.

Ha de demostrar el cumplimiento.

Otro principio; introduciendo en los considerandos el Acontability, documentar el cumplimientos.

4. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

Desde el diseño- La protección de datos ha de estar presente desde las primeras fases de elaboración del proyecto.

Por defecto- Solo se van a tratar aquellos datos personales que sean estrictamente necesarios para el fin del tratamiento.

5. EJERCICIO DE DERECHOS

- **Derecho de acceso.**

- **Derecho de rectificación**. Datos inexactos o incompletos.

- **Derecho de supresión** (derecho al olvido.). Cuando los datos no sean necesarios, cuando ya se cumpla el plazo legal.

- **Derecho de limitación**.- Mientras se resuelve solicitud del derecho de rectificación u oposición. Durante ese tiempo no se pueden tratar los datos.

- **Derecho de oposición**. Oponerme a un tratamiento.

- **Derecho de portabilidad.**

- **Derecho a no ser objeto de decisiones automatizadas**. Regla general es la prohibición, salvo que haya una previsión legal o se preste el consentimiento.

Respuesta en 1 mes. Puede ser en 2 por complejidad y número de solicitudes (esta prórroga y el motivo habrá de comunicarse al interesado).

La Administración ha de facilitar el ejercicio de estos derechos.

6. ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

Artículo 32 del RGPD obliga a los responsables a que lleven a cabo una valoración del riesgo de los tratamientos que realicen con la finalidad de establecer las medidas a aplicar.

¿Qué es un análisis de Riesgo?

Novedad del RGPD. Gestión del riesgo desde el diseño. (Responsabilidad proactiva)

GESTION DE RIESGOS.- 3 etapas o momentos:

1.- Identificación del riesgo.

2.- Evaluación.

3.- El tratamiento de los riesgos.

6. ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

1.- Identificación de amenazas y riesgos.

Una amenaza es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados en el tratamiento de sus datos personales. En materia de protección de datos nos encontraríamos básicamente con tres tipos:

- Acceso ilegítimo a los datos (confidencialidad). ¿qué pasaría si accede quien no debe?
- Modificación no autorizada de los datos. ¿qué sucedería si se alteran indebidamente esos datos?
- Eliminación o supresión de los datos. ¿qué sucedería si perdemos los datos?

El nivel de riesgo se mide según la probabilidad de que suceda y el impacto que tendría en caso de suceder.

5. ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

2.- Evaluar ese riesgo

¿Cómo valoramos el impacto? En función de los daños que puedan producirse si la amenaza se cumple: Sería mínimo o despreciable si no tiene consecuencias sobre el interesado o significativo si el daño ocasionado fuese grave.

.

6. ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

3.- Tratar los riesgos

Establecer medidas de control que permitan reducir la probabilidad de que los riesgos se materialicen.

Por tanto, con el análisis de riesgo determinaremos las medidas a aplicar para que los tratamientos cumplan con las disposiciones del Reglamento en atención al resultado del análisis.

Destacar que en los ayuntamientos con población inferior a 20.000 habitantes el análisis de riesgo se puede llevar a cabo con el soporte de la correspondiente Diputación Provincial.

La Agencia de Protección de Datos ha publicado una guía de ayuda.

6. ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

Es conveniente que se realice de forma metódica. Metodologías más utilizadas:

MAGERIT, CRAMM, PILAR

El RGPD no establece unas medidas de seguridad concretas.

Partiendo de un análisis de riesgos que valorará estos y determinara en función de los mismos las medidas de seguridad técnicas y organizativas a adoptar.

ENS, sigue siendo herramienta válido para gestión de riesgo y adoptar medidas de seguridad en las Administraciones.

Seudonimización- Disminuye el riesgo de los tratamientos.

7. EVALUACIONES DE IMPACTO

Si el Responsable constata que el tratamiento que se está realizando o se va a realizar entraña graves riesgos para los derechos y libertades de los interesados en lo que respecta a sus datos personales, deberá realizar una **EIPD**.

Es una **herramienta** que permite **evaluar** de manera **anticipada** cuáles son los **potenciales riesgos** y el **nivel de riesgo** a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos, y ello con el objetivo de establecer las medidas de control adecuadas para reducir ese riesgo hasta un nivel considerado aceptable.

RGPD señala también que cuando sea **probable** que un tipo de tratamiento (por utilizar nuevas tecnologías, por su alcance, contexto o fines,) entrañe un alto riesgo para los derechos y libertades, el responsable realizará, antes del tratamiento, una evaluación de impacto.

Herramienta de carácter preventivo, para poder identificar, evaluar y gestionar los riesgos a que están expuestas las operaciones de tratamiento, su objeto es garantizar los derechos y libertades de las personas físicas.

7. EVALUACIONES DE IMPACTO

CUÁNDO HAY QUE HACER UNA EVALUACIÓN DE IMPACTO

Estos supuestos se encuentran contemplados en el artículo 35 del RGPD.
El RGPD obliga cuando:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- Tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales.
- Observación sistemática a gran escala de una zona de acceso público.

7. EVALUACIONES DE IMPACTO

Para valorar si un tratamiento se realiza a gran escala debe tenerse en cuenta (según el Grupo del Artículo 29, en relación con la designación de Delegados de Protección de Datos):

a) El número de interesados afectados, bien en términos absolutos, bien como proporción de una determinada población

b) El volumen de datos y la variedad de datos tratados

c) La duración o permanencia de la actividad de tratamiento

d) La extensión geográfica de la actividad de tratamiento

Tratamientos anteriores a la aplicación del RGPD.- No tienen que hacer EIPD.

7. EVALUACIONES DE IMPACTO

Excepciones:

Cuando se hayan producido cambios en los riesgos que el tratamiento implica en relación con el momento en que el tratamiento se puso en marcha:

- Por aplicar nuevas tecnologías

- Que los datos se estén usando para finalidades distintas o adicionales a las que se decidieron en su momento

- Que se estén recogiendo más datos, o datos diferentes, de los que en principio se utilizaban para el tratamiento.

Por exigencia del Reglamento, las autoridades de control han de publicar un listado de actividades incluidas y excluidas de realizar una EIPD.

El listado es orientativo

8. QUIEBRAS DE SEGURIDAD

Qué es? El acceso no autorizado a los datos, la destrucción, pérdida o alteración, tanto ilícita como accidental.

El responsable debe notificarla:

1.- A la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

Plazo: sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.

Contenido mínimo:

a) la naturaleza de la violación

b) categorías de datos y de interesados afectados

c) medidas adoptadas por el responsable para solventar la quiebra

8. QUIEBRAS DE SEGURIDAD

d) si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados. Además, los responsables deben documentar las quiebras de seguridad sufridas (Tiene que haber un registro).

2.- A los afectados en los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los mismos.

Objetivo de la notificación a los afectados: permitir que puedan tomar medidas para protegerse de sus consecuencias.

Plazo: sin dilación indebida.

Contenido: recomendaciones sobre las medidas que pueden tomar los interesados para hacer frente a las consecuencias de la quiebra.

8. QUIEBRAS DE SEGURIDAD

Excepciones a la notificación a los afectados:

a) El responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado.

b) Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.

c) Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

Todo ello sin perjuicio de las obligaciones derivadas del Esquema Nacional de Seguridad.

8. QUIEBRAS DE SEGURIDAD

- **Quiebra por parte del encargado del tratamiento:**

Debe notificarlo al responsable sin dilación alguna. El responsable será quien deberá fijar las obligaciones de notificación del encargado.

- **Quiebras que pudieran tener gran impacto:**

Contactar con la autoridad de supervisión tan pronto como existan evidencias. Completar posteriormente la notificación formal completa.

Casos en que la notificación no pueda realizarse dentro de esas 72 horas por su complejidad.- Posibilidad de hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso.

La información puede proporcionarse de forma escalonada cuando no sea posible hacerlo en el mismo momento de la notificación.

Criterio de alto riesgo.- Es probable que la violación de seguridad ocasione daños de entidad a los interesados.

Ejemplos: contraseñas o participación en determinadas actividades, difusión de forma masiva datos sensibles o perjuicios económicos para los afectados.

Existe un canal para notificar a la Agencia las brechas de seguridad.

9. VIDEOVIGILANCIA

La imagen es un dato de carácter personal ya que identifica o hace identificable a una persona. Por ello, la instalación de cámaras, con diversas finalidades como podría ser la seguridad, el control laboral, el acceso a zonas restringidas captando la matrícula del coche y la imagen del conductor, o incluso la monitorización de una UVI, supondría un tratamiento de datos de carácter personal y en consecuencia, se le aplicaría la normativa de protección de datos.

Videovigilancia: sólo debe utilizarse cuando no sea posible acudir a otros medios que causen menos impacto en la privacidad.

No se pueden captar imágenes de la vía pública con fines de seguridad, ya que es competencia de las Fuerzas y Cuerpos de Seguridad (LO 4/1997, de 4 de Agosto) salvo el caso que:

- Resulte imprescindible para la finalidad que se pretende.

- Resulte imposible evitarlo por razón de la ubicación de las cámaras.

9. VIDEOVIGILANCIA

El tratamiento de videovigilancia debe constar en el Registro de actividades de Tratamientos.

Está prohibida la instalación en baños, vestuarios, o lugares análogos.

El tratamiento de las imágenes con fines de seguridad mediante la videovigilancia debe adecuarse al RGPD, de manera que en primer lugar, hay que configurar el registro de actividades de tratamiento regulado en el artículo 30 del RGPD y en el caso de las Administraciones públicas, y vinculado al principio de transparencia administrativa, su registro de actividades de tratamiento sí debe ser objeto de publicación, ya sea en la sede electrónica o en el correspondiente Portal de Transparencia.

9. VIDEOVIGILANCIA

Asimismo, se tiene que dar cumplimiento al derecho de información del artículo 13. Para ello se puede optar por un sistema de capas de la siguiente forma:

- Colocar un cartel donde aparezca que es una zona videovigilada, la identidad del responsable y la posibilidad del ejercicio de los derechos previstos en los artículos 15 a 22 del RGPD.

- Mantener a disposición de los afectados el resto de información referida en el artículo 13.

Se deberán adoptar las medidas de seguridad de conformidad con lo dispuesto en el artículo 32 del RGPD (medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo).

Esquema Nacional de Seguridad.- aplicable a cualquier información de las Administraciones Públicas sin distinción del soporte en el que se encuentre, por lo que en cuanto a las medidas de seguridad se refiere, este esquema es acorde al enfoque de riesgo del RGPD y se constituye en una herramienta válida para la gestión del riesgo y la adopción de las medidas de seguridad en las Administraciones.

9. VIDEOVIGILANCIA

La implementación de las medidas de seguridad cuando se lleve a cabo un tratamiento de datos mediante el uso de la videovigilancia dependerá del análisis de riesgo llevado a cabo previamente.

Si se encarga a un tercero la gestión de las cámaras.- encargado del tratamiento, quién deberá cumplir los requisitos que regula el artículo 28 del RGPD.

En todo caso, deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

El Estatuto de los Trabajadores faculta al empresario para adoptar las medidas que estime más oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, que deberán guardar la consideración debida a la dignidad humana y tener en cuenta la capacidad real de los trabajadores con discapacidad.

.

9.VIDEOVIGILANCIA

Los sistemas de videovigilancia para control empresarial sólo se adoptarán cuando exista una relación de **proporcionalidad** entre la finalidad perseguida y el modo en que se traten las imágenes y no haya otra medida más idónea.

Asimismo, se deberá informar personalmente a los trabajadores, o en su caso, a través de la representación sindical, por cualquier medio que garantice la recepción de la información.

El principio de minimización del artículo 5 del RGPD requiere que los datos personales tratados sean adecuados, pertinentes y limitados en relación con los fines para los que son tratados. Ello supone:

- Que el número de cámaras se limite a las necesarias para cumplir la función de vigilancia.

- Que el responsable analice también los requisitos técnicos de las cámaras, ya que el zoom o las denominadas "cámaras domo" pueden afectar y limitar al citado principio de minimización.

Asimismo, los monitores de grabación deben situarse de forma que, en la medida de lo posible, únicamente puedan ser visualizados por aquellos cuya función sea controlar los equipos que realizan las grabaciones, y no estar expuestos al público.

9. VIDEOVIGILANCIA

En aquellos supuestos en que las cámaras no graban imágenes pero sí se permite la reproducción en tiempo real de las mismas, también supone un sometimiento a lo dispuesto en el RGPD, debido a que existe un tratamiento de datos personales. De esta forma, hay que cumplir con la citada norma.

Entre las obligaciones que hay que adoptar estarían, por ejemplo, lo referente tanto al registro de actividades de tratamiento como el derecho el derecho de información, a los que nos hemos referido anteriormente.

Plazo de conservación establecido en el RGPD, máximo 1 mes, pasado el cual se suprimen, salvo en aquellos supuestos en que se deban conservar para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, y demás normativa específica en la materia, y con sujeción a lo dispuesto en la normativa de protección de datos.

Corresponderá a las Administraciones Públicas con competencia para la regulación del tráfico, autorizar la instalación y uso de estos dispositivos, adoptando una resolución a tal efecto.

CREMADES & CALVO-SOTELO

ABOGADOS

www.cremadescalvosotelo.com

Madrid • A Coruña • Barcelona • Granada • Málaga • Marbella • Pamplona • Sevilla
Bogotá • Buenos Aires • Casablanca • Ciudad de México • París • Santiago de Chile • Tel Aviv • Puerto Rico