Boletín 06/18

LOPD EN LA EMPRESA

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

Altabir consulting

EL RGPD UE 2016/679 EN APLICACIÓN

¿Por qué nos interesa el considerando 47?

Contenido

En el **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 datos personales y a la libre circulación de estos datos, en adelante (el RGPD), se descubren día a día nuevos elementos , como es el **considerando 47**.

En él se regula que **el interés legítimo del responsable del tratamiento**, incluso el de un responsable al que se puedan comunicar datos personales o de un tercero, nos servirá de base jurídica para el tratamiento, teniendo en cuenta siempre lo siguiente:

- **Que no prevalezcan los intereses** o derechos y libertades del interesado.
- **Que las expectativas del interesado sean razonables,** basadas en su relación con el responsable.

Así mismo, nos da un claro ejemplo de interés legítimo a aplicar **en la relación entre cliente/responsable**:

- Siempre y cuando existe una relación pertinente y apropiada entre el interesado y el responsable, tal y como sucede en las relaciones en las que el interesado es cliente o está al Servicio del responsable.

IMPORTANTE

*"El tratamiento de datos personales con **fines de mercadotecnia directa** puede considerarse realizado por **interés legítimo**",* cuando haya una relación previa cliente y responsable.

SANCIONES DE LA AEPD

Sanción por utilizar datos personales para una finalidad diferente para la que fueron recogidos

Los principios relativos al tratamiento deben ser observados cuidadosamente por el responsable.

Resolución AP/00104/2009 instruido por la AGPD **a la Diputación de Castellón** vista la denuncia presentada por D.A.A.A.

El denunciante manifiesta que es **policía local y que recibió una notificación de una multa de tráfico a su dirección del trabajo** sin que la Diputación lo hubiera intentando antes en el domicilio que consta en el fichero del Registro de vehículos, por lo que considera que **se ha hecho un uso indebido de una información de carácter personal**, tal y como es su condición de funcionario de Policía Local.

Realizando las actuaciones previas de investigación y esclarecimiento se tuvo conocimiento que el Ayuntamiento de Benicassim, **delegó a la Diputación de Castellón la gestión de multas de tráfico**, para ello, le envió un listado de los miembros del Cuerpo de Policía Local facultados para formular denuncias, **asignándoles como domicilio profesional, el domicilio del Ayuntamiento, al cual se envió la notificación de la multa.**

La Diputación, **no actuó diligentemente**, ya que según la *Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial*, las notificaciones de este tipo de procedimientos, **deben dirigirse primero al domicilio que conste en el Registro de Vehículos,** mientras que la Diputación **utilizó la base de datos del Ayuntamiento** para el envío de la multa.

La AGPD resolvió declarar que la Diputación de Castellón incurrió en una infracción tipificada como grave.

IMPORTANTE

art.4.2 de la LOPD "*los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para los que se hubieran recogido.*

LA AEPD ACLARA

Comunicación de imágenes al interesado

Interés Legítimo en la Videovigilancia

La cuestión planteada y resuelta por el gabinete jurídico, es si se puede, **comunicar a solicitud del usuario de un aparcamiento**, **las imágenes** de la matricula obtenidas con las videocámaras para ser prueba, en juicio, de los daños causados en su vehículo por otro usuario del aparcamiento.

Según el ***considerando 26 del Reglamento*** (UE) 2016/679 del Parlamento Europeo y del Consejo, (en adelante RGPD), "*los principios de protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable….*"
Además, **el art.4.1 del RGPD define *"datos personales"*** con una gran amplitud, considerando la matrícula del vehículo un dato que permite identificar directa o indirectamente a una persona.

La comunicación de datos que se pretende debe estar sujeta al principio de licitud del tratamiento del art.6 del RGPD, según la AGPD, **se ampara en el art.6.f**, ya que el tratamiento es necesario para la satisfacción del interés legítimo perseguido por el reclamante.

No obstante siempre debe de **realizarse la necesaria ponderación exigida**, y amparándose, en este caso, en **la Ley de Enjuiciamiento Civil/2000**, el **ejercicio del derecho a la tutela judicial efectiva y a la defensa de la persona** que solicita los datos **prevalece** sobre el derecho a la protección de datos personales.

IMPORTANTE

Para la comunicación de las imágenes, se tendrá también en cuenta el principio de minimización de datos.

ACTUALIDAD LOPD

La AEPD presenta una guía para gestionar y notificar las quiebras de seguridad según el Reglamento.

Fuente: AEPD

(Madrid, 19 de junio de 2018). La Agencia Española de Protección de Datos (AEPD) ha presentado hoy la 'Guía para la gestión y notificación de brechas de seguridad' junto a ISMS Forum y en colaboración con el Centro Criptológico Nacional (CCN) e INCIBE. El objetivo de este documento es ofrecer a las organizaciones tanto recomendaciones preventivas como un plan de actuación, de forma que conozcan cómo evitarlas y cómo proceder en caso de que se produzcan.

El Reglamento General de Protección de Datos (RGPD) define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Con anterioridad a la aplicación del RGPD, la obligación de notificar a la Agencia las brechas de seguridad que pudiesen afectar a datos personales se ceñía exclusivamente a operadores de servicios de comunicaciones electrónicas y prestadores de servicios de confianza. Desde el pasado 25 de mayo, **esta obligación pasa a ser aplicable a cualquier responsable de un tratamiento de datos personales**, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

De acuerdo con el Reglamento, cuando el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe notificarlo sin dilación a la autoridad de control competente, y a más tardar en las 72 horas siguientes a haber tenido constancia de ella. Esta notificación a la Agencia debe realizarse a menos que sea improbable que dicha brecha de la seguridad constituya **un riesgo para los derechos y las libertades** de las personas físicas.

Puede ver más información en el siguiente enlace:

Guía para la gestión y notificación de brechas de seguridad

EL PROFESIONAL RESPONDE

Cómo legitimar el tratamiento de datos de contacto de las personas que prestan sus servicios en la empresas y autónomos

En relación con **este tipo de datos**, tenemos que considerar que **no están excluidos de la regulación del Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación (en adelante RGPD), los cuáles ***no aparecen en ninguna*** de ***las no aplicaciones del art.2.2*** del RGPD que recoge el ***"ámbito de aplicación material".***

Estos datos (nombre, teléfono, e-mail...) son de carácter personal, ya que podemos determinar la identidad de una persona a través de esos identificadores.

Según el **art.4.2, el tratamiento de estos datos** por ejemplo, recogida, registro, organización y consulta, **tendrán que tener una base legítima**. Así en virtud **del principio de licitud del art.6.1f, es el Interés legítimo del responsable,** siempre y cuando éste no prevalezca sobre los intereses o derechos fundamentales del interesado que requiera la protección de datos personales.

No obstante, se deberá cumplir con el resto de preceptos del Reglamento, como son los **principios relativos al tratamiento del art.5 del RGPD** y en concreto los que hacen relación a:

Limitación de la finalidad: recogidos con fines determinados, explícitos y legítimos.

Minimización de datos: adecuados pertinentes y limitados a lo necesario en relación a los fines para los que son tratados.

IMPORTANTE

El Responsable tiene que cumplir con los principios relativos al tratamiento del art. 5 RGPD y además, ser capaz de demostrarlo, en virtud del principio de responsabilidad proactiva.