Boletín 04/20

LOPD EN LA EMPRESA

Balaguer & Gutiérrez
Correduría de Seguros
Consultoría de Protección de Datos

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

EL RGPD UE 2016/679 EN APLICACIÓN

Los Principios de Protección de datos

Todas y cada una de las actuaciones que lleva a cabo el responsable respecto del tratamiento de los datos personales se tienen que realizar teniendo en cuenta lo dispuesto en la normativa y, en especial, cumpliendo los principios de protección de datos.

¿Cómo se deben tratar entonces los datos personales por los responsables y encargados de tratamiento?

Se han de tratar de forma lícita, leal y transparente en relación con el interesado, este sería el principio de licitud, lealtad y transparencia, dando una información adecuada. Los fines para los que se recojan tendrán que ser determinados y explícitos y además no se pondrán utilizar para otros diferentes, este es el principio de limitación de la finalidad**. El principio de minimización requiere que los datos recogidos sean los adecuados, pertinentes y limitados a lo necesario para el cumplimiento de los fines**. Por ejemplo, en un formulario de potenciales clientes, no solicitaremos más datos que los necesarios para enviar información. Los datos tienen que ser exactos y si fuera necesario actualizarlos. Además, se tienen que mantener sólo durante un plazo de tiempo determinado necesario para los fines del tratamiento. **Todo ello, garantizando al interesado una total integridad y confidencialidad de sus datos.**

Contenido

IMPORTANTE

El responsable debe cumplir todos los principios de protección de datos y además ser capaz de demostrarlos (ppº de responsabilidad proactiva)

SANCIONES DE LA AEPD

Los comercios electrónicos que no cumplen con la normativa son sancionados por la AEPD

En el procedimiento sancionador https://www.aepd.es/es/documento/ps-00469-2019.pdf instruido por la AEPD, se sanciona al responsable del comercio electrónico SOLO EMBRAGUE, S.L. por no cumplir con los requisitos establecidos en la normativa que regula el comercio electrónico, la Ley34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, conocida como (LSSI) y los requisitos del RGPD.

El reclamante, un particular que accedió a la página web para solicitar un presupuesto, reclama ante la AEPD que el titular de la página web recaba datos personales a través de un formulario de contacto, sin que en ningún apartado se pueda acceder a la política de privacidad y conocer quién es el responsable del tratamiento. Por tanto, se vulnera el cumplimiento del deber de informar del art.13 del RGPD. La multa en este aspecto ascendió a 1.500 euros.

Por otro lado, tampoco cumplía con la información requerida en la LSSI, puesto que no existía ningún banner que informara de la utilización de cookies, ni tampoco links que redirigieran a una política de cookies. Esta infracción es tipificada como leve en el artículo 38.4 g de la LSSI, pudiendo ser sancionada con una multa de hasta 30.000€. En esta ocasión la sanción impuesta fue de 1.500 euros, teniendo en cuenta la intencionalidad y el plazo de tiempo de la infracción.

Las reclamaciones ante la AEPD han ido creciendo exponencialmente desde que entró en aplicación el RGPD.

IMPORTANTE

La LOPDGDD considera muy grave la omisión del deber de informar al afectado acerca del tratamiento de sus datos personales.

LA AEPD ACLARA

Informe sobre el tratamiento de datos en relación con el COVID-19

En este informe la AEPD da respuesta a la legitimación de los tratamientos de datos de salud en relación con el COVID-19. https://www.aepd.es/es/documento/2020-0017.pdf

El RGPD en su considerando (46) recoge que, en situaciones excepcionales, como una pandemia, la base jurídica de tratamientos puede ser múltiple. Partiendo de la exigencia del reglamento, para el tratamiento de los datos de salud, no basta una base jurídica, sino que además ha de existir una circunstancia que levante la prohibición del tratamiento, siendo éstas las siguientes:

1º Entre el empleador y empleado cumplimiento de obligaciones y derechos en el ámbito del Derecho laboral y de la seguridad y protección social, según lo dispuesto en la normativa de prevención de Riesgos Laborales. No solamente debe velar por la prevención el empleador, sino también el trabajador. En el ámbito de la situación actual del COVID-19 supone que el trabajador debe informar a su empleador si sospecha de contacto con el virus, con el objetivo de salvaguardar su salud y la de los demás trabajadores del centro de trabajo.

2º El tratamiento es necesario por razones de un interés público esencial y un interés público en el ámbito de la salud pública como protección frente a amenazas transfronterizas.

3ºEs necesario para realizar un diagnóstico medico o asistencia de tipo sanitario y gestión de los sistemas de asistencia sanitaria y social.

IMPORTANTE

Para el tratamiento de los datos se aplicarán los principios del RGPD, en especial, los principios de minimización de datos y finalidad.

ACTUALIDAD LOPD

Campañas de phishing sobre el COVID-19

Fuente: AEPD

Mientras dure la situación de alerta los ciberdelincuentes aprovecharán para lanzar ataques de phishing y de todo tipo para sacar provecho.

El modus operandi será siempre muy similar: los ciberdelincuentes tratarán de suplantar organizaciones legítimas con información relevante sobre el COVID-19 como el Ministerio de Sanidad, una Consejería de Sanidad de una Comunidad Autónoma, Fuerzas del Orden, Organizaciones Internacionales, simulando prestar ayuda y consejo, o incluso fingiendo ser la empresa en la que trabajas. Lo harán a través de mensajería instantánea como WhatsApp o Telegram y también a través de emails. En la mayoría de los casos te pedirán que abras un archivo con urgencia o sigas un enlace de internet para obtener la información.

Si se sigue el enlace y se descarga y ejecuta un archivo adjunto, se tratará de algún tipo de malware que permita a los ciberdelincuentes tomar el control de tu dispositivo, acceder a tu información y datos personales e incluso cifrar esos datos.

Los enlaces de internet incluidos en estos mensajes o correos electrónicos también te pueden llevar a páginas web que suplantan la identidad de otras organizaciones para robar tus credenciales de acceso a un servicio u otra información personal, por ejemplo, tu número de la seguridad social, los datos bancarios para el pago de un test de coronavirus, etc.

Sigue las siguientes recomendaciones:

- Mantente informado mediante fuentes oficiales y confiables, acudiendo directamente a las webs de las instituciones o medios de comunicación, nunca a través de un enlace proporcionado en un mensaje o en un email.
- Verifica la dirección de correo electrónico remitente del mensaje y también el enlace web al que te remite el mensaje. A veces, resulta obvio que la dirección web no es legítima, pero otras veces los ciberdelincuentes son capaces de crear enlaces que se parecen mucho a las direcciones legítimas.
- Ten cuidado con las solicitudes de datos personales a través de webs a las que has llegado siguiendo un enlace contenido en un mensaje o correo electrónico. Mejor accede directamente a la web de esa organización.

Puede ver más información en los siguientes enlaces

Campañas de Phising sobre el COVID-19

Guía de privacidad y seguridad en Internet

EL PROFESIONAL RESPONDE

¿Tienen los responsables que seguir notificando a la AEPD las brechas de seguridad durante el estado de alarma?

Recientemente se publicaba en nuestro País el Real Decreto 463/2020 que establecía en España el estado de alarma para combatir la situación de Pandemia originada por el COVID-19. En la disposición adicional tercera de este decreto, se indica lo siguiente "se suspenden términos y se interrumpen los plazos para la tramitación de los procedimientos de las entidades del sector público".

¿Se supone entonces que los responsables y encargados del tratamiento de datos tienen que suspender las comunicaciones de brechas de seguridad ocurridas durante este plazo de tiempo?

La respuesta sería negativa. En este caso en concreto no afecta esa suspensión. Al contrario, es ahora más que nunca, cuando las entidades deben de mostrar su lado más proactivo y poner todos los medios que tengan a su alcance para hacer frente a los peligros y amenazas que puedan ocasionar ciberataques en nuestra entidad. Según la AEPD, las notificaciones de las brechas de seguridad proporcionan información que permiten a las Autoridades de Control y los ciudadanos aplicar las medidas necesarias, generando confianza en el uso de la nuevas tecnologías y seguridad de la información.

En el caso de que la brecha de seguridad no cumpla los criterios para su notificación a la AEPD tenemos que registrarla en el registro de incidencias y aplicar las medidas que sean necesarias.

IMPORTANTE

El plazo para notificar las brechas de seguridad a la Autoridad de Control es de 72 horas desde que se tiene conocimiento de la brecha de seguridad.