Boletín 08/20

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

Responsable del tratamiento y encargado del tratamiento

La normativa en protección de datos, en concreto el RGPD y nuestra Ley Orgánica LOPDGDD, define las obligaciones y responsabilidades de cada uno de los principales sujetos en el tratamiento de los datos.

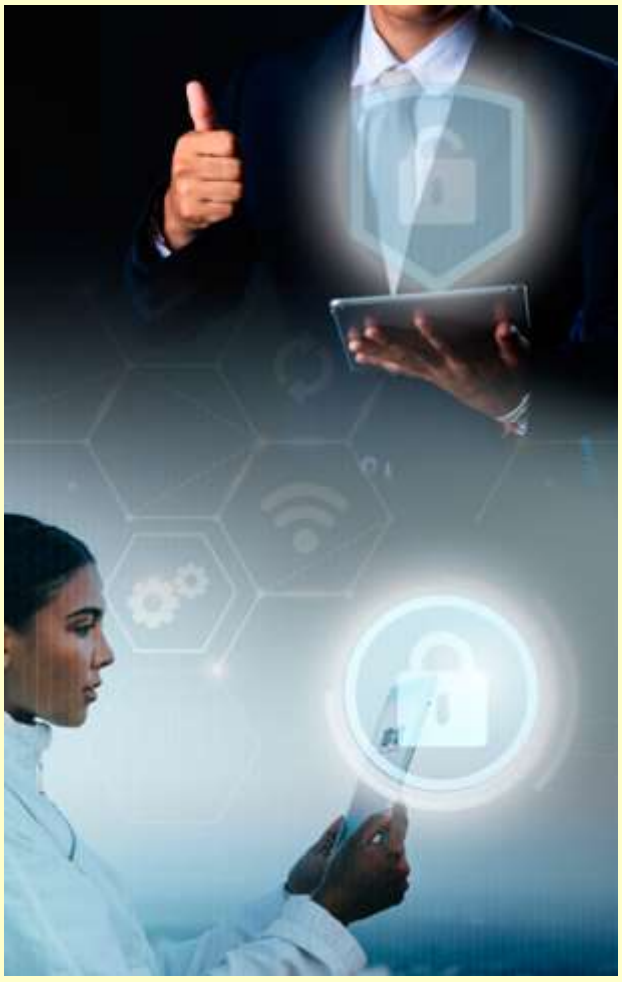
En el art.4 del RGPD se define al responsable del tratamiento, como aquella persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento. Por otro lado, el encargado es aquella persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales siguiendo las instrucciones del responsable.

En la LOPDGDD existe un apartado, denominado "disposiciones aplicables a tratamientos concretos", en el cual, la normativa indica cómo tienen que actuar el responsable y encargado en relación con los datos personales y esos tratamientos.

En sucesivos boletines los iremos desarrollando:

1º Tratamiento datos de contacto de empresarios.
2º Sistemas de información crediticia.
3º Videovigilancia.
4º Sistemas de exclusión publicitaria.
5º Información de denuncias internas.

Contenido



IMPORTANTE

Es obligatorio que el responsable y encargado de tratamiento tengan bien cumplimentado y actualizado el registro de actividades del tratamiento.

SANCIONES DE LA AEPD

Sancionada con 6.000 euros una entidad por no notificar a sus clientes ni a la AEPD el hackeo a su cuenta de correo

En el procedimiento sancionador https://www.aepd.es/es/documento/ps-00122-2020.pdf instruido por la AEPD, se sanciona a SAUNIER-TEC, MANTENIMIENTOS DE CALOR Y FRIO, S.L.(el reclamado), por no notificar una brecha de seguridad. La sanción impuesta fue de 6.000 euros.

La reclamante presenta escrito de reclamación ante la AEPD alegando que había recibido una serie de emails solicitando una serie de cambios en sus datos personales, incluyendo su número completo de cuenta bancaria. El dominio desde el cual le llegó el correo tenía una extensión diferente, lo que indicaba que no eran emails oficiales enviados por la empresa SAUNIER-TEC. **La reclamante se puso en contacto con la entidad para conocer de la brecha de seguridad y no recibió respuesta del responsable de protección de datos.**

La AEPD a la vista de los hechos, admite a trámite la reclamación e inicia el procedimiento sancionador contra la entidad por infringir los artículos 33 y 34 del RGPD, los cuales regulan cómo y cuándo ha de notificarse la brecha de seguridad que puedan suponer un riesgo para los derechos y libertades de las personas físicas. **En este caso, la AEPD determina que, dada la categoría de datos afectados, datos bancarios y el número de afectados por la brecha, se tendría que haber notificado a los afectados.**

La comunicación al interesado se debe realizar utilizando un lenguaje claro y sencillo.

IMPORTANTE

El responsable ha de notificar a la AEPD las brechas de seguridad antes del plazo de 72horas desde su conocimiento.

LA AEPD ACLARA

¿Puede un establecimiento registrar los datos de los clientes que acuden a un local de ocio?

La AEPD ha publicado el día 31-07-2020 un comunicado en el que trata de analizar diversas iniciativas públicas para conseguir una reacción rápida ante los posible nuevos brotes de COVID-19. **Una de ellas es registrar determinados datos de los clientes que acudan a un local de ocio.**

En primer lugar, señala que los datos recogidos no son datos de salud, por lo tanto, no pueden englobarse en la categoría de datos especiales.

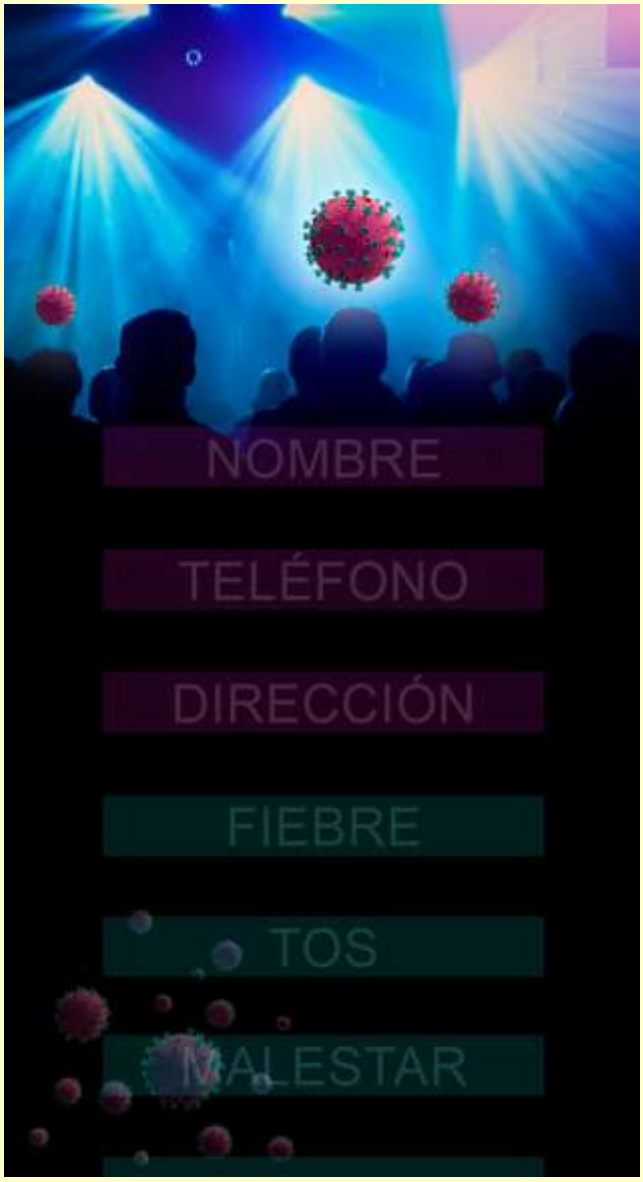
En segundo lugar, la necesidad de aplicar dicha medida debe ser acreditada por las autoridades sanitarias y, además, ser obligatoria puesto que sino perdería su efectividad. En el caso de que la legitimación para el tratamiento fuera el consentimiento del interesado, éste no tendría que suponer ninguna consecuencia negativa, como es el caso de impedir la entrada al establecimiento.

La AEPD viene a determinar que la base jurídica, con carácter preferente, sería el art.6.1.C del RGPD, el tratamiento es necesario para el cumplimiento de una misión realizada en interés público de controlar la pandemia.

En el comunicado se dan una serie de pautas para llevar a cabo el tratamiento:

Justificar la medida: Identificar en qué tipo de establecimiento es necesaria.

Minimizar datos: recoger solamente el número de teléfono del interesado, junto con los datos del día y la hora de asistencia al lugar.



IMPORTANTE

El Comité Europeo de Protección de Datos recomienda la anonimización y la minimización de datos en las aplicaciones de seguimiento de contactos en el contexto de la pandemia.

ACTUALIDAD LOPD

La AEPD actualiza su Guía sobre el uso de cookies para adaptarla a las nuevas directrices del Comité Europeo

Fuente: AEPD

(Madrid, 28 de julio de 2020). La Agencia Española de Protección de Datos (AEPD) ha actualizado la Guía sobre el uso de las cookies para adaptarla a las Directrices sobre consentimiento modificadas en mayo de 2020 por el Comité Europeo de Protección de Datos (CEPD). La nueva versión de la Guía realizada por la Agencia ha contado, tal y como ocurrió con versiones anteriores, con la participación de los sectores afectados (las asociaciones ADIGITAL, Asociación Española de Anunciantes, AUTOCONTROL e IAB Spain).

El Comité Europeo de Protección de Datos ha revisado en mayo de 2020 las Directrices 05/2020 sobre consentimiento con el fin de aclarar su posición en relación con dos cuestiones: la validez de la opción "seguir navegando" como forma de prestar el consentimiento por parte de los usuarios y la posibilidad de utilizar los conocidos como "muros de cookies", es decir, de limitar el acceso a determinados servicios o contenidos sólo a los usuarios que acepten el uso de cookies.

En relación con el primero de estos puntos, el Comité considera que la opción de "seguir navegando" no constituye en ninguna circunstancia una forma válida de prestar el consentimiento, en la medida en que tales acciones pueden ser difíciles de distinguir de otras actividades o interacciones del usuario, por lo que no sería posible entender que el consentimiento es inequívoco.

Respecto a los "muros de cookies", el Comité ha precisado que, para que el consentimiento pueda considerarse otorgado libremente, el acceso al servicio y a sus funcionalidades no debe estar condicionado a que el usuario consienta el uso de cookies.

Por ello, la Guía explicita que no podrán utilizarse los denominados "muros de cookies" que no ofrezcan una alternativa al consentimiento. Este criterio resulta especialmente importante en aquellos supuestos en los que la denegación de acceso impediría el ejercicio de un derecho legalmente reconocido al usuario, por ser, por ejemplo, el acceso a un sitio web el único medio facilitado al usuario para ejercitar tal derecho.

Podrán existir determinados supuestos en los que la no aceptación de la utilización de cookies impida el acceso al sitio web o la utilización total o parcial del servicio, siempre que se informe adecuadamente al respecto al usuario y se ofrezca una alternativa de acceso al servicio sin necesidad de aceptar el uso de cookies.

Puede ver más información en el siguiente enlace

Guía sobre el uso de las cookies

Directrices 05/2020 sobre consentimiento

EL PROFESIONAL RESPONDE

¿Cuáles son las consecuencias de la cancelación del Privacy-Shield?

El Tribunal de Justicia Europeo (TJUE) ha declarado en su sentencia la invalidez de la Decisión 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. conocido como Privacy-Shield.

Son muchas las preguntas que como responsables del tratamiento de los datos nos surgen a raíz de esta sentencia. Por ejemplo, ¿puedo seguir utilizando los servicios en la nube facilitados por proveedores americanos? ¿qué debemos tener en cuenta para que éstas cumplan la normativa europea?

Las transferencias internacionales podrán realizarse bajo la celebración de las Cláusulas contractuales tipo de la Decisión 2010/87, que regulan los contratos de acceso a datos por cuenta de terceros ya que éstas no han sido invalidadas por el TJUE. En cuanto a la utilización de estas Cláusulas, el CEPD está estudiando incorporar medidas adicionales para garantizar un nivel de protección adecuado. Mientras tanto, se deja en manos del responsable (el exportador de datos) la valoración, entre otros requisitos, las medidas de seguridad aportadas por el proveedor de servicios.

El CEPD insta a utilizar mecanismos de excepción del art. 49RGPD, por ejemplo, el consentimiento del interesado. Este debe ser explícito, específico para esa transferencia e informado de los riesgos de la falta de protección adecuada.

IMPORTANTE

En el apartado de Transferencias internacionales de la AEPD se puede encontrar toda la información relativa a la supresión del Privacy-Shield.