Boletín 07/22

LOPD EN LA EMPRESA

EL RGPD UE 2016/679 EN APLICACIÓN

Tratamientos concretos: Sistemas exclusión publicitaria

Los sistemas de exclusión publicitaria son aquellos que permiten a los ciudadanos evitar recibir comunicaciones comerciales.

El tratamiento de los datos personales de aquellos que hayan manifestado su negativa u oposición a recibir dichas comunicaciones comerciales estará legitimado en el interés público, tal y como establece nuestra Ley Orgánica, la LOPDGDD. Estos sistemas, que pueden tener carácter sectorial o general, solamente incluirán los datos imprescindibles para identificar a los afectados.

Las entidades responsables de estos sistemas se lo comunicarán a la autoridad de control competente que lo publicará en su sede electrónica. **En la actualidad, solamente existe un fichero de exclusión publicitaria que está gestionada por la Asociación Española de Economía Digital. Este sistema se conoce como la Lista Robinson.**

El artículo 23 de la LOPDGDD que regula este sistema, da indicaciones de cómo ha de llevarse a cabo este tratamiento por las entidades responsables. Así, cuando un interesado manifieste que no quiere seguir recibiendo comunicaciones comerciales, deberá informarle de la existencia de los sistemas de exclusión publicitaria.

Contenido

IMPORTANTE

Cuando se vaya a realizar una campaña de mercadotecnia directa se deberán consultar estos sistemas para excluir aquellos que hayan manifestado su negativa.

SANCIONES DE LA AEPD

Un laboratorio es sancionado con 20.000€ por comunicar los resultados del test COVID-19 de una trabajadora

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00323-2021.pdf se sanciona a un laboratorio por comunicar los resultados del test COVID- 19 de una trabajadora a su responsable en el Ayuntamiento.

La reclamación la interpuso una trabajadora de un Ayuntamiento alegando que los resultados de anticuerpos COVID-19 que le fueron realizados por un "laboratorio privado" se los comunicaron por correo electrónico, incluyendo, además, en el correo, la dirección de su responsable en el Ayuntamiento. Esta cesión se hizo sin el consentimiento de la trabajadora.

La AEPD, en sus actuaciones de investigación, solicitó al laboratorio privado evidencias de la información que se daba a las personas a las que se les tomaban las muestras. **El laboratorio contestó manifestando que se les informó verbalmente de las pruebas a realizar y la finalidad de éstas.** Además, alegó, que "por error logístico, se suponía que el consentimiento informado con el paciente se realizaba en el Ayuntamiento, por lo que, no se recogió en el momento de la muestra, por ser una prueba voluntaria".

El laboratorio es sancionado con 20.000€. Como responsable del tratamiento de los datos de salud debería de haber recogido expresamente el consentimiento de los afectados.

Cada vez hay una mayor conciencia entre los interesados en la protección de sus datos personales.

IMPORTANTE

El responsable del tratamiento debe aplicar todas las medidas técnicas y organizativas posibles para garantizar la integridad y confidencialidad de los datos personales.

LA AEPD ACLARA

Los servicios de vigilancia de la salud son responsables de informar al trabajador/a de la comunicación de sus datos

En el informe del Gabinete Jurídico de la AEPD se da respuesta a una consulta planteada por una empresa prestadora del servicio de vigilancia de la salud.

En algunas ocasiones, estas entidades tienen que comunicar al empresario determinada información sobre sus trabajadores/as. Es el caso, cuando se solicitan servicios extras, como determinadas vacunas o ampliación de reconocimientos. Estos servicios deben ser abonados por el empresario cuando se encuentren dentro del catálogo de servicios que los empleados/as tienen derecho a solicitar.

En este informe se da respuesta a la legitimación para realizar la comunicación de los datos de salud al empresario. **Así, el RGPD permite una excepción para el tratamiento de estos datos sin necesitar el consentimiento del afectado cuando se trata del cumplimiento de una obligación impuesta en el ámbito del Derecho laboral y de la seguridad y de la protección social, como es este caso.**

En la normativa que regula la prevención de riesgos laborales, se establece el derecho de los trabajadores/as a una protección eficaz en materia de seguridad y salud en el trabajo. El empresario está obligado a elaborar y conservar a disposición de la autoridad laboral la documentación relativa a los controles del estado de salud, por lo que podrá tener conocimiento de aquellos que requieran servicios extras. **La información de esta comunicación al trabajador/a debe hacerla la entidad que presta el servicio de vigilancia de la salud.**

IMPORTANTE

Se comunicarán los datos que estrictamente sean necesarios para determinar la actividad de vigilancia de la salud a la que se han sometido en cada caso en concreto.

ACTUALIDAD LOPD

Metaverso y privacidad

Fuente: AEPD

Desde el punto de vista de la privacidad, el uso del metaverso puede ser muy intrusivo, ya que el conjunto de datos que se tratan aumenta de forma exponencial. Cualquier entorno virtual está plenamente datificado desde su diseño y permite tratar un espectro más amplio de información relativa a actividades humanas.

Los metaversos pretenden ampliar la experiencia de las redes sociales mucho más allá del aspecto visual o de los gráficos en 3D. El metaverso involucra al usuario en múltiples dimensiones, como la social, económica, política o emocional, hasta virtualizar todos los aspectos de desarrollo del individuo, y extiende los datos recogidos a la información no verbal y biométrica. La coyuntura colectiva y técnica actual ha creado el contexto ideal para su desarrollo y expansión, traduciendo las experiencias humanas a un tratamiento de datos digitales mediante simulaciones. Sin embargo, el tratamiento de estos datos personales es completamente real.

Los mundos virtuales o metaversos llevan mucho tiempo presentes en la literatura y cine de ficción. Hasta ahora, las redes sociales eran una proyección del metaverso sobre un entorno lineal y con una capacidad limitada de penetración en el resto de las dimensiones que conforman nuestra realidad. Sin embargo, en la actualidad el metaverso ya no se trata de una utopía y se está avanzando en su implementación. Esto es posible gracias a que ya se dispone de la masa crítica de tecnologías y condicionantes sociales que permiten su despliegue con opciones de obtener una rentabilidad económica.

Por un lado, el marco de la pandemia ha acelerado el despliegue de servicios, a todos los niveles, sobre plataformas digitales. Además, y lo que es más importante, se ha dado un salto de gigante en la penetración de estos servicios en todos los segmentos de la población, en particular en las personas más jóvenes. Dos de estos servicios son críticos: aquellos que involucran la interacción social, y la aceptación masiva de los medios de pago digitales.

Por otro lado, las tecnologías que permiten desplegar una vida virtual ya se encuentran maduras y todas ellas permiten una interacción inmersiva en los espacios virtuales, que conceden al usuario una experiencia social, una identidad digital y una propiedad de activos con un mercado de intercambio. Las aplicaciones son infinitas, tantas como actividades humanas: mercados de productos digitales, descentralización de las finanzas, eliminación de intermediarios, juegos, educación, trabajo, interacción social, diseño y simulación, salud, compra de terrenos digitales, etc.

No se trata de teorías o futuribles, sino que ya existen conocidas compañías con proyectos…

Puede ver más información en el siguiente enlace:

Metaverso y privacidad

EL PROFESIONAL RESPONDE

Seguridad en el correo electrónico corporativo: Política de seguridad (II)

La política de seguridad del correo electrónico corporativo, tal y como veíamos en el anterior boletín, tiene que ponerse a disposición de todos los usuarios/as de dispositivos digitales en la empresa y asegurarse de que conocen su contenido.

Así, por ejemplo, en lo que respecta al uso del correo electrónico corporativo, se incorporará en la política de seguridad que se ha de desactivar la ejecución de macros y la descarga de imágenes los correos electrónicos. Este formato permite incluir un lenguaje de programación denominado *JavaScript*, que puede ser utilizado con fines ilícitos, por ejemplo, para verificar que nuestra cuenta de correo es válida o para redirigirnos a un sitio web malicioso.

Otra de las medidas que se pueden incluir en esta política de seguridad del correo electrónico es ofuscar las direcciones de correo electrónico corporativo. Estas direcciones no deben ser publicadas en páginas web o redes sociales sin utilizar técnicas de ofuscación, ya que estas cuentas podrían ser captadas para incluirlas en listas de envío de spam.

Es muy importante también, advertir sobre la inspección de los enlaces. Antes de hacer clic, el receptor debe revisar la URL, situándose sobre el texto del enlace para visualizar la dirección del envío.

IMPORTANTE

Cuando se reciba un mensaje con un adjunto analizar si el icono se corresponde con el tipo de archivo y la extensión no contenga espacios en blanco.

AUTOR: JULIO CÉSAR MIGUEL PÉREZ