RESUMEN NOTICIAS DE ACTUALIDAD EN PROTECCIÓN DE DATOS Y BOLETÍN LOPD EN LA EMPRESA

AÑO 2022

Software y Servicios para Asesorías y Empresas

Consultores en Protección de Datos (RGPD-LOPD)

Empresa Colaboradora

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España,** es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

PRODASUR

Consultores en Protección de Datos (RGPD-LOPD)

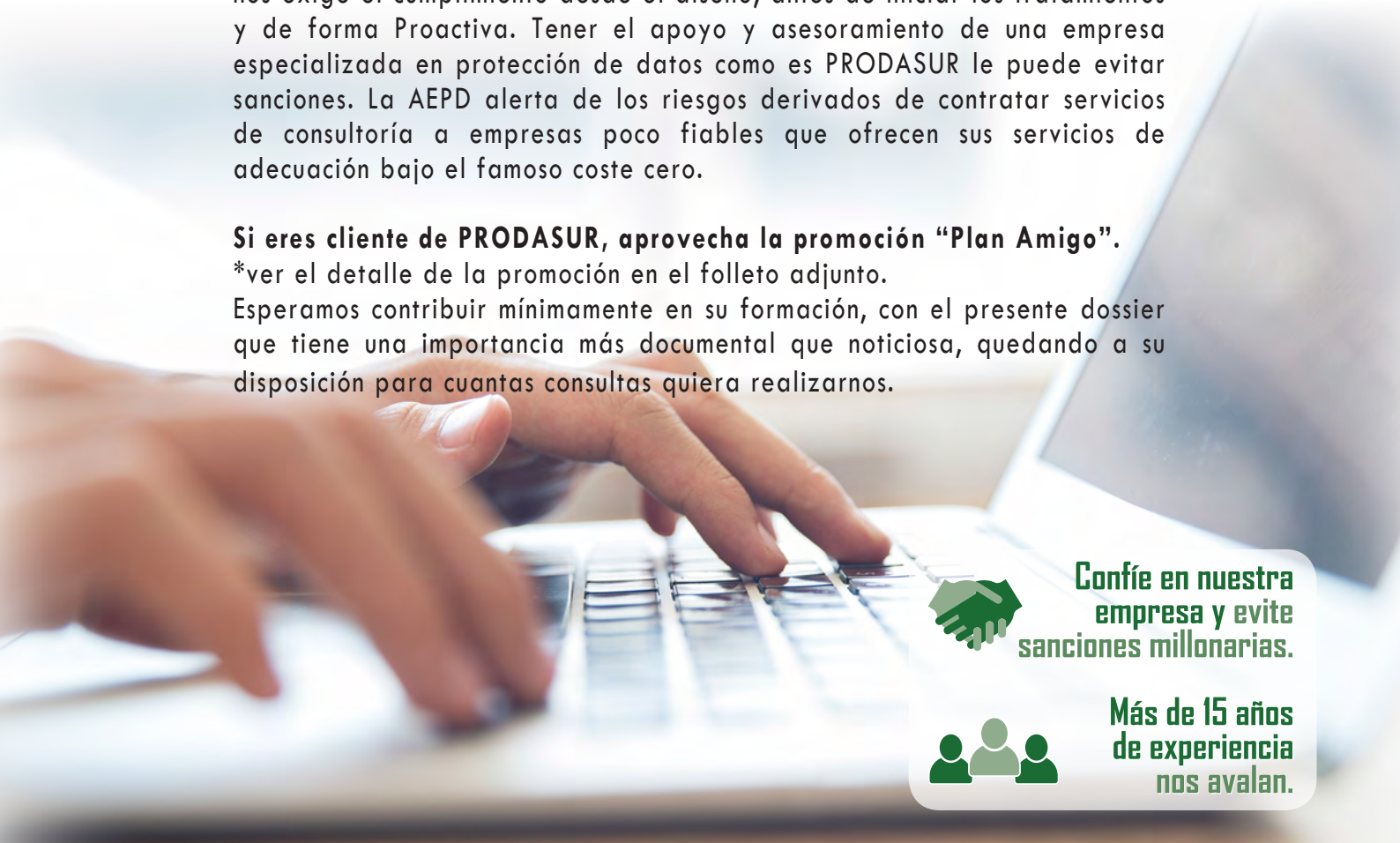
PRESENTACIÓN:

El presente "Dossier RGPD y LOPD-GDD" tiene un carácter informativo, y es nuestra pretensión ofrecer una orientación respecto a la aplicación de la normativa de protección de datos. Son numerosas las cuestiones legales que podríamos abordar, siendo solo una mínima parte las seleccionadas.

Ofrecemos extractos sobre el RGPD y LOPD-GDD que son relevantes en el día a día para garantizar con su aplicación el cumplimiento de lo establecido en la normativa vigente y evitar posibles sanciones en materia de protección de datos.

Queremos destacar la importancia de disponer de un proyecto dirigido al cumplimiento de la normativa en materia de protección de datos: La norma nos exige el cumplimiento desde el diseño, antes de iniciar los tratamientos y de forma Proactiva. Tener el apoyo y asesoramiento de una empresa especializada en protección de datos como es PRODASUR le puede evitar sanciones. La AEPD alerta de los riesgos derivados de contratar servicios de consultoría a empresas poco fiables que ofrecen sus servicios de adecuación bajo el famoso coste cero.

Si eres cliente de PRODASUR, aprovecha la promoción "Plan Amigo".
*ver el detalle de la promoción en el folleto adjunto.
Esperamos contribuir mínimamente en su formación, con el presente dossier que tiene una importancia más documental que noticiosa, quedando a su disposición para cuantas consultas quiera realizarnos.



Confíe en nuestra empresa y evite sanciones millonarias.

Más de 15 años de experiencia nos avalan.

EMPRESA REGISTRADA incibe

ApCpD

apep Asociación Profesional Española de Privacidad

PRODASUR es miembro del **Instituto Nacional de Ciberseguridad de España,** de la **Asociación Profesional de Consultores en Protección de Datos** y de la **Asociación Profesional Española de Privacidad** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo).

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

www.prodasur.es

prodasur@prodasur.es

Avda. Comandante Benítez, 15 Local 2 · 29001 Málaga
Atención al Cliente: 952 60 37 70 - 902 15 22 25

ENERO

11/01/2022 Las multas por Protección de Datos aumentan un 521% durante 2021. FUENTE: eleconomista.es

El importe de las multas impuestas por las autoridades de control europeas derivadas del incumplimiento del Reglamento General de Protección de Datos, superó la barrera de los mil millones de Euros en 2021. Esta cantidad de sanciones supone un aumento del 521% en comparación con el volumen de sanciones impuesto en el año 2020.

Este pasado año se ha impuesto un total de 412 sanciones, aunque las sanciones más altas han sido las que se impusieron de un lado, por parte de la autoridad luxemburguesa, a Amazon Europe Core, por importe de 746 millones de Euros; y, por otro lado, la que la autoridad irlandesa impuso a Whatsapp, que alcanzó los 225 millones de Euros.

Al hacer un análisis comparativo de la intensidad sancionadora de los organismos de control, en el año 2020, el montante total de las multas superó los 171 millones de Euros, lo que supuso un incremento significativo en comparación con los 72 millones de Euros del año 2019.

Lejos quedan los 436.000 euros en multas del año 2018, año en cuyo mes de mayo comenzó a aplicarse la citada normativa en todos los estados miembros.

Estos datos, sin duda, consolidan al riesgo sancionador como una de las principales preocupaciones de las empresas y de sus órganos de administración, destaca Francisco Pérez Bes, Socio de Derecho Digital en Ecix Group y antiguo Secretario General del Instituto Nacional de Ciberseguridad de España (INCIBE), y requiere mantener, de manera constante, un alto nivel de cumplimiento especializado dentro de las organizaciones, añade.

La exigencia de cumplimiento de una norma tan compleja y exigente como es el RGPD, sin duda ha aumentado el nivel de cumplimiento de las empresas, aunque, a la vista de los datos publicados, parece que las organizaciones todavía están lejos de alcanzar un nivel de cumplimiento adecuado. Ahora bien, no pueden negarse los esfuerzos de las empresas por cumplir con esta normativa, por lo menos en España.

Sin embargo, España es uno de los países de la Unión Europea que acumula una mayor cantidad de multas en comparación con el resto de nuestros vecinos. En concreto, la Agencia Española de Protección de Datos ha impuesto, este pasado año, 352 multas, lo que se ha traducido en sanciones por valor de 36,7 millones de Euros. Esto supone una sanción media de 105.000€ .

A la vista de los datos publicados, las violaciones más comunes pueden estructurarse en cinco grandes grupos. El mayor volumen se centra en incumplimientos de los principios generales de protección de datos, a lo que sigue la falta o insuficiente información facilitada a los titulares de los datos. En tercer lugar, destaca la insuficiente base legitimadora para el tratamiento de los datos personales. Finalmente, encontramos a las sanciones relacionadas con brechas de seguridad y, por consiguiente, con la ausencia de

medidas técnicas u organizativas adecuadas en la organización afectada, son el grupo que mayor evolución está teniendo, especialmente a la vista del incremento -tanto en número

como en complejidad- de ciberataques a empresas, en particular, ransomware. Y, por último, encontramos la deficiente gestión de los derechos ejercidos por los ciudadanos -comúnmente conocidos como derechos Arco+- en aquellas organizaciones que tratan datos personales de personas físicas.

La gestión de los datos en las empresas es una tarea muy compleja. La información se ha convertido en un activo estratégico, cada vez mas valioso, a la par que la asunción de riesgo por su deficiente protección es cada vez mayor. Además, el riesgo regulatorio y sancionador para 2022 va a ser todavía mayor, año en el que se prevé una mayor intensidad en ciberataques y un mayor impacto reputacional de todo aquello relacionado con la ciberseguridad y la protección de los datos personales. Así las cosas, podemos afirmar que la exigencia del regulador para este año también va a ir en aumento, al igual que ocurrirá con las reclamaciones económicas de los afectados por brechas de datos y violaciones de seguridad y, previsiblemente, contra los órganos de administración de las empresas que hayan sufrido incidentes de seguridad, advierte Pérez Bes.

La Comisión Europea actualizó el año pasado sus reglas para las transferencias internacionales de datos. Bruselas refuerza así su normativa, que ahora exige más control en el traslado de los datos y carga con nuevas obligaciones a las empresas que envíen fuera de la Unión Europea esta información. El Ejecutivo comunitario adoptó el pasado 4 de junio las nuevas cláusulas contractuales tipo.

La Comisión Europea ha publicado una consulta pública sobre la próxima Ley europea de libertad de los medios de comunicación, una iniciativa anunciada por la presidenta von der Leyen para salvaguardar la integridad, el pluralismo y la independencia de los medios de comunicación en el mercado interior. La consulta abarca tres grandes ámbitos: transparencia e independencia; condiciones para su buen funcionamiento; y la asignación equitativa de recursos estatales. Bruselas presentará la propuesta en el segundo semestre de 2022.

14/01/2022. Piden a Protección de Datos que aclare si el uso de las cookies de Google Analytics conlleva una transferencia de datos a EEUU, lo que vulneraría el RGPD. FUENTE: businessinsider.es

Noyb, una plataforma en defensa de la privacidad de los internautas europeos, ha logrado que el Supervisor Europeo de Protección de Datos (EDPS) aperciba al Parlamento Europeo por alojar una página web con cookies de Google Analytics. La razón: Noyb entiende que esas cookies suponían de facto una transferencia internacional de datos personales.

El presidente de Noyb es el austríaco Max Schrems. Su activismo le ha convertido en una auténtica pesadilla para grandes tecnológicas como Facebook, e incluso su apellido bautiza dos sentencias del Tribunal de Justicia de la Unión Europea sobre las que se ha amparado el EDPS para cerrar el caso contra la Eurocámara.

Es la última de estas dos, la sentencia Schrems-II (de verano de 2020) la que hacía caer el Privacy Shield. Este Privacy Shield no era otra cosa que un acuerdo entre EEUU y

Bruselas para garantizar la transferencia de datos personales de los usuarios, algo para lo que el Reglamento General de Protección de Datos exige suma minuciosidad.

Sin embargo, en Schrems-II el Tribunal de Justicia de la UE consideraba que el nivel de protección de datos personales en EEUU era problemático y no era proporcional a la protección que sí se garantiza en el Viejo Continente. A tenor del fallo judicial, Noyb inició procedimientos contra más de 100 empresas europeas ante las autoridades de protección de datos de distintos países miembros.

Las primeras resoluciones se han conocido esta semana. La primera, del EDPS, contra la propia Eurocámara. La segunda, este miércoles, de la autoridad de protección de datos austríaca, que dictaminó que Google Analytics viola el RGPD, como detalla la plataforma Noyb en su web y recogen medios como la agencia Efe.

Esta última detalla que en el proceso ante la autoridad de control austríaca, Google admitió que "todos los datos recogidos a través de Google Analytics (...) se alojan en EEUU".

De ser así, y de cundir este ejemplo al resto de autoridades de protección de datos europeas, la aplicación de la sentencia Schrems-II tendría finalmente un efecto "en el mundo real", como reivindica el propio Schrems en un comunicado de su organización, al tiempo que generaría mucha inseguridad jurídica, opina Gonzalo Oliver Martín.

Gonzalo Oliver es asesor jurídico en materia de Protección de Datos, Privacidad y Ciberseguridad, trabaja en OZONIA Consultores y es socio de la Asociación Española de Delegados de Protección de Datos (aeDPD). Este mismo miércoles elevó un escrito a la propia Agencia Española de Protección de Datos instándola a emitir un informe jurídico sobre este tema.

La AEPD tendrá que pronunciarse
Protección de Datos, aunque ahora está inmersa en el proceso de selección para su primera Presidencia (que sustituirá a la interina directora general, Mar España, en las próximas semanas), tendrá que emitir un informe jurídico. Gonzalo Oliver tiene muchas dudas en torno a esta controversia, y no es el único incapaz de dar una respuesta clara y contundente a una sencilla pregunta:

¿Transfiere datos Google a EEUU cuando recoge las cookies de Analytics?

Analytics es una herramienta de métrica de audiencias que permite a los responsables de distintos sitios web comprobar cuántos usuarios (y audiencias) entran en sus portales y cómo interactúan con él. Vozpópuli señaló que el Gobierno de España estaría inclumpliendo la Schrems-II porque, al igual que el Parlamento Europeo, utiliza Analytics en sus páginas.

Sin embargo, esta herramienta también está presente en un sinfín de páginas de empresas de marketing, en tiendas electrónicas, y en la práctica totalidad de los medios de comunicación españoles.

En su resolución, el Supervisor Europeo de Protección de Datos tan solo apercibía al Parlamento Europeo porque se trata de una institución pública. Pero si los organismos de protección de datos siguen su ejemplo, las sanciones económicas por vulnerar el RGPD podrían acabar llegando a las empresas de distintos estados miembros.

Noyb, en el más de centenar de denuncias que presentó ante estos organismos de control, incluyó las páginas de compañías españolas como la startup malagueña Freepik e incluso de entidades como la Real Academia Española.

"A mí me extraña mucho que el Reglamento de Protección de Datos se aprobara en 2016, se aplicara en 2018, cayeran los Privacy Shield de la UE con EEUU, ¿y ahora 5 años después se dan cuentas de que se siguen haciendo transferencias internacionales de datos a través de las cookies de Google Analytics?", se pregunta Gonzalo Oliver.

Oliver es el firmante de un escrito que dirigió a la AEPD esta semana para que se pronunciara con un informe jurídico para tratar de salvar la inseguridad que ha suscitado tanto la resolución del EDPS como la posterior resolución de la agencia austríaca. "En caso de investigarse o sancionarse a Google, debería ser la DPC, la agencia irlandesa".

Esto se debe a que Irlanda es el país en el que se asientan las matrices de varias grandes tecnológicas, entre ellas de la propia Google. "Tienen una filial en España, pero está destinada a la venta de servicios", recuerda. Así, la AEPD no sería la autoridad competente para tratar el asunto de estas cookies, pero sí se puede pronunciar para tratar de arrojar algo de luz a esta problemática.

"Otra cosa que a mí me extraña: Google tiene seis servidores en Europa. Esos centros de datos se ubican Irlanda, dos en Países Bajos, Dinamarca, Finlandia y Bélgica". "¿Todas las cookies de empresas de marketing, de medios, todas se van a enviar a EEUU? ¿No hay ninguna que se quede almacenada en los servidores que Google tiene en Europa?".

De confirmarse que absolutamente todas las cookies de Google Analytics que usan las administraciones y empresas de toda Europa suponen un traslado de datos personales a EEUU, supondría una hecatombe. Y abriría dos escenarios: uno, en el que la sanción económica la asumiría Google, u otro peor:

Uno en el que la sanción económica iría a las empresas que utilizan esta herramienta de métrica de audiencias, asestando un gravísimo golpe a muchas compañías emergentes que al calor de la pandemia se han animado a digitalizar buena parte de sus negocios.

Sobre la resolución de la autoridad de control austríaca, el propio Schrems, presidente de Noyb, se congratulaba de la misma: "En lugar de adaptar sus servicios al RGPD, muchas empresas estadounidenses han intentado simplemente incluir unas líneas de texto a sus políticas de privacidad, ignorando el fallo del Tribunal de Justicia de la Unión Europea".

Como expone Gonzalo Oliver en su escrito a Protección de Datos: "Muchos responsables del tratamiento se encuentran desorientados ante estas últimas noticias y la decisión tomada por el Supervisor Europeo". Lo seguirán estando hasta que no haya una respuesta.

14/01/2022. El 2022 año del dato personal. FUENTE: cincodias.elpais.com

2022 será un año con grandes retos para la protección de datos. Los procesos legislativos en la Unión Europea incidirán en el marco regulador actual y abrirán interrogantes significativos sobre su encaje con el Reglamento General de Protección de Datos (RGPD). Sin perjuicio del largo trámite de la ePrivacy Regulation, hay que considerar la **Data Governanc**e Act, la legislación sobre servicios digitales, y la regulación de la inteligencia artificial. Además, la estrategia europea de digitalización implica construir espacios sectoriales europeos de datos. Simultáneamente, en el plano tecnológico confluyen blockchain, privacidad diferencial, entornos de tratamiento para la analítica de datos (data spaces) federados o centralizados, y la inteligencia artificial.

De otro lado, las estrategias nacionales en protección de datos han puesto sobre la mesa cuestiones que deberían ser tenidas en cuenta ya que la homogeneidad buscada por el reglamento puede verse en riesgo. Los criterios de las autoridades de protección de datos nacionales no siempre coinciden, se incrementa el volumen sancionador y se aprecia asimetría en la regulación de los elementos disponibles del RGPD en el nivel nacional. A ello se suma que las autoridades, en términos de plantilla y de toma de decisiones, poseen distintas capacidades y políticas.

Adicionalmente, resulta necesario incluir un elemento de carácter sustancial. El conjunto de los Estados de la Unión va a afrontar un ciclo de intensa transformación digital e innovación de la mano de los fondos de reconstrucción. Y España va a ser el primer país en afrontar el reto. Este ciclo innovador va a ser altamente dependiente de los modelos de cumplimiento normativo en protección de datos. Por ello, resultará estratégico un enfoque económico del derecho capaz de conjugar las garantías de los derechos, la investigación, la innovación y el emprendimiento.

El estado del arte en protección de datos puede influir de modo decisivo a la hora de la toma de las decisiones empresariales o del sector público. En este sentido, el carácter defensivo o proactivo de los equipos de compliance, a su vez altamente dependiente de los pronunciamientos de los reguladores, puede ser determinante para generar velocidades de innovación y trasformación digital asimétricas en los distintos estados de la Unión.

Lo mismo sucede desde el punto de vista del sector público. Aquí, no solo se trata de la ejecución de los fondos europeos. El Covid ha impulsado un nuevo ciclo de innovación y desarrollo del sector público más allá del tan citado teletrabajo. La pandemia ha puesto en valor el Estado social de derecho y ha puesto de manifiesto la necesidad de migrar hacia un modelo de generación de políticas públicas basadas en los datos.

Así pues, las futuras acciones del Gobierno y las Administraciones serán, sin duda, dependientes de procesos decisionales basados en una intensa analítica de datos. Y ello nos enfrenta al reto de transformar profundamente el modo en el que las Administraciones

procesan la información personal y adoptan decisiones que afectan a la ciudadanía. Por otra parte, la trasposición de la directiva Open Data y las previsiones de la Data Governance Act abocan a la definición de nuevas estrategias de reutilización de los datos del sector público al servicio del bien común.

Por último, 2022, vuelve, una vez más, a poner en valor el carácter esencial para nuestro futuro del ecosistema de los profesionales de la privacidad, y nos exige un enfoque proactivo y de innovación responsable. No olvidemos que nuestro horizonte consiste en proteger personas y, por paradójico que resulte, deberíamos plantearnos con rigor si la respuesta más funcional a este desafío exige a su vez nuevos enfoques.

Ricard Martínez Martínez, director de la Cátedra de privacidad y Transformación Digital Microsoft-Universitat de Valencia.

14/01/2022. Confirmada la sanción a una empresa que dio un microcrédito a una persona que suplantó una identidad. FUENTE. Expansión.com

La empresa denunciada incurrió en dos infracciones graves de la Ley de Protección de Datos por tratar datos personales sin recabar el consentimiento de las personas afectadas y por vulnerar la exigencia de exactitud y veracidad de los datos.

La sección tercera de la sala de lo contencioso del Tribunal Supremo ha confirmado una sanción de 80.000 euros que impuso la Agencia de Protección de Datos a una empresa que concedió un microcrédito 'online' a una persona que suplantó la identidad de otra.

En concreto, la Agencia de Protección de Datos impuso la sanción a la empresa Dineo Crédito S.L. por vulnerar la Ley de Protección de datos, ya que la persona que solicitó el microcrédito aportó el Documento Nacional de Identidad (DNI) de otra persona.

Finalmente, el dinero del crédito no se devolvió y Dineo incluyó al titular del DNI suplantado en una lita de morosos. El hombre cuya identidad fue suplantada denunció la situación ante la Agencia de Protección de Datos, ya que entendía que Dineo trató sus datos personales sin su consentimiento.

La Agencia de Protección de Datos concluyó que Dineo, la empresa denunciada, había incurrido en dos infracciones graves de la Ley de Protección de Datos por tratar datos personales sin recabar el consentimiento de las personas afectadas y por vulnerar la exigencia de exactitud y veracidad de los datos, al haber incorporado en sus sistemas informáticos los datos del denunciante y dando traslado de ellos al fichero de solvencia patrimonial Asnef.

Así, el nombre del denunciante figuraba en la lista de morosos asociado a una deuda de 161 euros, deuda que no era cierta, vencida ni exigible ya que el denunciante no había contratado el microcrédito.

Ahora, el Tribunal Supremo ha rechazado el recurso de casación de la empresa y ha confirmado la sentencia de la Audiencia Nacional que también confirmó, a su vez, la sanción de 80.000 euros impuesta por la Agencia de Protección de Datos.

En su sentencia, el Supremo explica que comparte el criterio de la Audiencia Nacional sobre la insuficiencia de las medidas que aplicó Dineo en el procedimiento de contratación 'online' del microcrédito, en tanto que "se desentienden enteramente del

objetivo de verificar la veracidad y la exactitud de los datos, y, en particular, de comprobar que quien solicita el crédito es precisamente quien dice ser".

La sentencia de la Audiencia Nacional explicaba que, en el proceso de contratación la plataforma de la empresa, se exigía determinados datos, como el número del DNI, dos teléfonos y el correo electrónico. Unos datos que "se ignora si son del cliente que los facilita como suyos o si son de otras personas".

En relación con el DNI, su validación consistía en un algoritmo que permite determinar si el DNI facilitado por el cliente se corresponde o no con un DNI real o válido. Pero dicha medida "únicamente demuestra" a la entidad que "alguien es titular de ese DNI, por cuanto le confirma que es un número de documento que existe".

Asimismo, la sentencia del Supremo aprecia que de este modo, "en cualquier caso en el que un tercero utilice indebidamente un DNI sustraído o extraviado para realizar una compra o solicitar un crédito 'online', siempre se consumaría el tratamiento inconsentido de los datos personales del titular del documento, aunque éste hubiese denunciado en su día ante las autoridades la pérdida o sustracción de su DNI, pues ninguna de las medidas enunciadas por la recurrente aparece mínimamente orientada a impedir o dificultar que ese resultado se produzca".

Por último, el TS señala que lo anterior no significa que se haga recaer sobre la empresa contratante la responsabilidad de impedir que se produzca un hecho ilícito o delictivo como es el uso fraudulento de un DNI por parte de quien no es su titular.

"Pero sí es exigible a dicha empresa contratante, como diligencia necesaria para que no se le pueda reprochar el incumplimiento de sus obligaciones en materia de protección de datos de carácter personal --tanto en lo que se refiere a la exigencia de consentimiento del interesado como en lo relativo al principio de veracidad y exactitud de los datos-- la implantación de medidas de control tendentes a verificar que la persona que pretende contratar es quien dice ser, esto es, que coincide con el titular del DNI aportado", concluye.

26/01/2022. Cómo gestionar tus derechos ante la recepción de publicidad no deseada. FUENTE: aepd.es

A pesar de actuar de manera responsable a la hora de dar mis datos, no dar consentimiento para que los traten con finalidades publicitarias, inscribirme en la Lista Robinson y de haber seguido todos los consejos para prevenir la publicidad no deseada que presentábamos en esta entrega anterior de nuestro blog, es posible que sigas recibiendo algún tipo de comunicación comercial no deseada a través de llamadas de teléfono, mails, sms o mensajes a través de aplicaciones de mensajería instantánea.

A continuación, te presentamos una serie de consejos o acciones que puedes realizar para limitar la publicidad no deseada:

Utiliza las fórmulas que te ofrecen

Las comunicaciones electrónicas publicitarias ofrecen sistemas para que puedas rechazar el uso de tus datos con fines publicitarios, que incluyen medios como el envío de un correo electrónico a la dirección electrónica indicada, un SMS, un enlace o la opción de llamar a un número telefónico gratuito.

Esta suele ser la manera más sencilla de dejar de recibir las comunicaciones comerciales de esa empresa, entidad u organización. Utilízala antes de pasar al resto de acciones que te presentamos.

Retira tu consentimiento
Si diste tu consentimiento cuando contrataste o te inscribiste en un servicio para que tratasen tus datos con fines publicitarios, puedes revocarlo en cualquier momento utilizando el método que la empresa ponga a tu disposición.

Si desconoces o no encuentras la manera de hacerlo, puedes consultar el apartado dedicado a la protección de datos de su página web.

Ejerce tu derecho de oposición
Puedes ejercer este derecho ante la entidad responsable del tratamiento para solicitar que te excluya de las campañas publicitarias que realice. Si lo haces, indica claramente en la solicitud que no deseas que traten tus datos con fines publicitarios e informa del canal por el que estás recibiendo la publicidad y los datos que no deseas que se traten. Por ejemplo, si recibes publicidad telefónica, puedes indicar tu número de teléfono para que no lo utilicen con fines comerciales.

En el espacio dedicado a los derechos de nuestra web dispones de más información sobre el mismo y formularios tipo para ejercerlo ante el responsable.

Ejerce tu derecho de supresión
Si no quieres que una entidad que te envía publicidad tenga tus datos, puedes ejercer tu derecho de supresión para que los elimine. Si eres cliente de la entidad, te recomendamos que optes por ejercer el derecho de oposición o retires el consentimiento prestado para que no continúe tratando tus datos con fines publicitarios.

En el espacio dedicado a los derechos de nuestra web dispones de más información sobre tu derecho de supresión y formularios tipo para ejercerlo ante la entidad responsable.

Contacta con el delegado de protección de datos
Gran parte de las discrepancias relacionadas con la protección de datos, también con la publicidad no deseada, se suelen resolver tras una comunicación o consulta al delegado de protección de datos de la organización, entidad o empresa que trata tus datos.

Dependiendo del tipo de entidad, esta puede estar obligada o no a disponer de un DPD, aunque muchas cuentan con uno de manera voluntaria. Puedes buscar si una entidad cuenta con un DPD y su contacto en la herramienta Consulta DPD de nuestra Sede Electrónica.

Reclama ante la Agencia

Si has realizado todo lo antes mencionado y el responsable del tratamiento no ha atendido a tus peticiones en los plazos estipulados o no has quedado satisfecho con su respuesta, puedes reclamar en la Agencia.

Este trámite se puede realizar de manera telemática a través de la Sede Electrónica de la Agencia. Para que podamos ayudarte debes adjuntar toda la documentación relacionada con el caso:

Registro, copia o captura de las comunicaciones recibidas.
Documentación que acredite tu inscripción en la Lista Robinson si es el caso.
Pruebas de haber intentado retirar tu consentimiento.
Comunicaciones realizadas con el delegado de protección de datos si lo hubiera.
Documentos que acrediten haber ejercido tus derechos de oposición y/o supresión, así como la respuesta recibida por el responsable del tratamiento.
Cualquier otro documento o prueba que pueda ser de utilidad para resolver la reclamación.
Recuerda que si lo que buscas es algún tipo de indemnización deberás acudir a los tribunales de justicia.

Valora la mediación
De manera adicional e independiente a todo lo indicado anteriormente, puedes optar por la mediación para resolver los conflictos relacionados con la publicidad no deseada. Muchas compañías, entre las que se encuentran la mayoría de las empresas de telecomunicaciones, están adheridas al sistema de mediación voluntaria y gratuita de Autocontrol. Encontrarás toda la información el servicio de mediación de Autocontrol en su página web.

Además, dispones de más información sobre cómo evitar la publicidad no deseada en el espacio dedicado a este tema de la web de la Agencia, en este vídeo de nuestro canal de YouTube y en esta infografía.

31/01/2022. Amazon, WhatsApp y Google lideran el ranking de las mayores multas de la UE por violar la protección de datos. FUENTE: larazon.es

El incumplimiento de la normativa RGPD puede conllevar sanciones de hasta 20 millones de euros o el 4% de la facturación global de una compañía. Hasta septiembre de 2021, las multas ascienden a más de 1.000 millones de euros

El incumplimiento del Reglamento General de Protección de Datos (RGPD) puede conllevar multas de hasta 20 millones de euros o el 4% de la facturación global de una compañía. En 2021, y hasta septiembre, la cantidad total de multas asciende a más de

1.000 millones de euros, siendo Amazon, la empresa a la que mayor multa se le ha impuesto, seguida por WhatsApp y Google. Así lo recoge EAE Business School en su estudio "La evolución del dato: Del big data a la inteligencia artificial".

El reglamento regula la protección de las personas respecto a sus datos personales y la circulación de estos datos en todo el territorio europeo, que entró en vigor en 2016 y se aplica desde 2018, tal y como se recoge en el estudio de EAE. Este reglamento asegura

los derechos de los usuarios en la recogida de datos, la introducción de derechos como el derecho al olvido, la limitación de su tratamiento y de los datos, obligación de hacer un análisis de los riesgos o el consentimiento de los usuarios, entre otros.

En julio de 2021, Amazon recibió la mayor multa de la historia de la Unión Europea en materia de privacidad: 746 millones de euros. La sanción fue impuesta por la autoridad de protección de datos de Luxemburgo, donde Amazon tiene la sede en Europa. Le siguió WhatsApp tan solo un mes y medio después, el 2 de septiembre de 2021, con una multa de 225 millones de euros por incumplir la normativa y, en concreto, por no proporcionar a los usuarios y no usuarios la información suficiente sobre cómo comparte los datos con Facebook, su empresa matriz. Hasta que la UE impuso estas dos sanciones, la más alta la ostentaba Google, obligada a pagar 50 millones de euros en 2019. El gigante tecnológico fue multado por el organismo francés encargado de hacer valer la protección de datos por "falta de transparencia, información incorrecta y ausencia de consentimiento válido en la publicidad personalizada".

Las multas de Amazon y WhatsApp dispararán la media de sanciones de 2021, ya que en 2020 las multas solo ascendieron a 158,5 millones, y según los datos recopilados hasta enero de 2021, el total de sanciones por incumplimiento del RGPD desde que se puso en marcha la normativa ascendía a 272,5 millones de euros.

"El hecho de que las empresas tengan una información sobre los usuarios que, antes no tenían, y herramientas como el big data para explotarla abre la puerta a considerar dónde queda el usuario ubicado en esta situación. Determinar si el big data es beneficioso para los usuarios es una tarea muy compleja. En algunos casos permite la existencia de ciertos servicios útiles pero, por otro lado, un mal uso del big data puede dar pie a abusos de los derechos de los usuarios", advierte Pau Sabaté, coautor del estudio de EAE Business School.

Los retos del big data: consumo eléctrico y discriminación social
La irrupción del ecosistema digital ha generado de forma exponencial una cantidad de datos que parece no tener límite ni frenar su creación. En los últimos 5 años, se ha multiplicado por cuatro la cantidad de datos digitales creados o replicados en todo el mundo, y se estima que para el 2025 se al menos doblará esta cifra, tal y como recoge el informe de EAE Business School.

El coste energético del big data es otro tema a abordar. El consumo eléctrico de todos los data centers juntos ya representa un 1% de la demanda global de electricidad.

Otro de los campos donde el big data está más inmaduro es en entender y gestionar el impacto que tiene a nivel social. Por ejemplo, tal y como señala el estudio, los sistemas de recomendación pueden crear burbujas informativas donde la gente sólo recibe información de la parte de la sociedad cercana a su ideología, a modo de sesgo de auto confirmación. Los sistemas de recomendación también son susceptibles de ser utilizados para difundir noticias falsas.

Otro riesgo puede ser la concesión de una hipoteca. Al lanzar el modelo predictivo, puede dar menos posibilidades de financiación a un perfil social determinado, y por tanto de desarrollo, creando una posible desigualdad social.

FEBRERO

03/02/2022. Protección de datos multa con 5,81 millones a varias operadoras por duplicados fraudulentos de tarjetas SIM. FUENTE: elespanol.com

El 'SIM Swapping' es un tipo de fraude que consiste en obtener un duplicado de una tarjeta SIM asociada a una línea de teléfono sin el consentimiento de su titular con el fin de suplantar su identidad y acceder a información confidencial, como redes sociales, servicios de mensajería instantánea, correos electrónicos o incluso aplicaciones bancarias.

Además de obtener esta información, con un duplicado de la tarjeta los delincuentes pueden recibir los SMS con los códigos de confirmación que permiten realizar determinadas operaciones por Internet, como compras online, transferencias o solicitudes de préstamos, y aprovecharse de ello para estafar al verdadero titular de la línea.

Tras recibir denuncias de varios particulares y la aparición de distintas noticias en los medios de comunicación en torno a este tipo de prácticas delictivas, la Asociación Española de Protección de Datos (AEPD) inició hace algo más de dos años una investigación para determinar la responsabilidad de los operadores de telecomunicaciones en este tipo de fraudes.

Un procedimiento del que han salido varios expedientes sancionadores contra distintos operadores de telecomunicaciones, a los que se les han puesto varias multas por una cuantía total de 5,81 millones de euros al considerar la AEPD que las políticas de seguridad que tienen estas compañías han sido insuficientes para evitar los duplicados fraudulentos.

En concreto, la agencia considera que estas compañías han cometido una "infracción muy grave" a la hora de gestionar el tratamiento de los datos que les proporcionan sus clientes, según lo recogido en el Reglamento General de Protección de Datos, así como en la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

Sanción desproporcionada
Desde las operadoras rechazan estas acusaciones y afirman que también se ven perjudicadas, junto con sus clientes, por la acción de los ciberdelincuentes. Un perjuicio que, añaden, se ve agravado por esta sanción "desproporcionada" que también afecta a su imagen pública y a la relación con sus clientes.

"La sanción impuesta por la AEPD es claramente desproporcionada, atendiendo al número de supuestos en que este tipo de fraudes llegan a materializarse, por lo que se trata de incidentes excepcionales que no pueden poner en duda los altos estándares de seguridad con los que se tratan los datos personales de los clientes", señalan a EL ESPAÑOL - Invertia.

En este sentido, inciden en que el objetivo principal de los delincuentes con el 'SIM Swapping' es poder acceder a las claves de confirmación para la realización de transferencias bancarias, cuyo diseño de seguridad es responsabilidad de las entidades bancarias y en el que las operadoras de telefonía no intervienen ni tienen relación alguna.

Además, añaden que la perpetración de este tipo de delitos requiere de la obtención previa, mediante engaño, de las claves bancarias de la víctima (habitualmente mediante técnicas conocidas como phishing), "por lo que responsabilizar a las operadoras por la comisión de estos delitos es improcedente".

Sin embargo, remarcan que, aunque la mejora del diseño de la seguridad de los procesos es responsabilidad de los bancos y entidades de crédito, continuarán "actualizando y reforzando sus protocolos de forma continua" para mejorarlos y optimizarlos con el objetivo de hacer frente a las cada día más complejas y diversas amenazas que los delincuentes desarrollan contra la seguridad de la información.

Vodafone recibe la sanción más alta

De todas las operadoras, Vodafone es, con diferencia, la que ha recibido la sanción administrativa más elevada, 3,94 millones. En su informe, la AEPD tiene en cuenta no sólo la investigación de oficio de las medidas adoptadas por Vodafone con carácter general por la compañía, sino también nueve reclamaciones presentadas por particulares ante la agencia.

En ellas, varios clientes de la operadora denuncian duplicados de tarjetas de personas ingresadas en hospitales o realizados en provincias distintas a las de residencia. Operaciones que en uno de los casos denunciados permitieron a los delincuentes sustraer 17.265,00 euros de una cuenta corriente, según los denunciantes.

En su resolución, la AEPD considera que queda probado que la política de seguridad de Vodafone ha resultado insuficiente para la adecuada protección de los derechos fundamentales de las personas cuyas tarjetas SIM han sido fraudulentamente duplicadas y señala que los datos recabados muestran que esta política no falla sólo en casos aislados como argumenta la operadora. De hecho, acusa a la compañía de tener una conducta "reactiva" y no "proactiva", tal y como exige el RGPD.

"Tal y como se ha probado, estas medidas de seguridad no eran adecuadas ni suficientes, pues la cesión de datos a terceros se ha producido sin verificar de forma fehaciente la identidad de los interesados", incide la agencia, que considera que terceros ajenos a los titulares de los datos han superado las medidas de seguridad establecidas en "múltiples ocasiones".

Tras conocer la resolución, Vodafone asegura que la AEPD ha valorado el caso "de forma errónea", pues parte de únicamente nueve reclamaciones interpuestas por particulares y extrae como consecuencia que las políticas de seguridad de la compañía estarían fallando.

En este sentido, afirma que aplica medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en todos sus canales, así como que ha sido proactiva en la implantación de medidas encaminadas a impedir duplicados SIM fraudulentos.

Además, agrega que ha realizado, de manera continua, evaluaciones de riesgo, así como revisiones y actualizaciones de medidas de seguridad. También recalca que ha colaborado con la propia AEPD en el marco del grupo de trabajo 'Duplicidad Tarjetas SIM' constituido por dicha Agencia.

En conclusión,considera que la sanción impuesta es "totalmente desproporcionada", teniendo en cuenta que trabaja de manera continua para asegurar que las operaciones se realizan de una manera segura y ha implementado de forma proactivas medidas para ello, así como que "no existe negligencia o intencionalidad alguna por parte de Vodafone".

Multas a Telefónica, Orange y MásMóvil
La segunda multa más elevada son los 900.000 impuestos a Telefónica por los datos recabados tanto en la investigación de oficio como en tres reclamaciones presentadas ante la AEPD. Por ejemplo, en una de ellas un usuario denuncia que, como consecuencia del duplicado fraudulento de su tarjeta, se realizaron dos transferencias de 28.000 euros desde sus cuentas, mientras que otro afectado alerta de dos ingresos en Revolut por importe total de 6.000 euros.

La AEPD también considera que en esos casos ha quedado demostrado que Telefónica no ha cumplido los principios relativos al tratamiento de los datos personales afectados. "No basta con disponer de una política de seguridad, sino que hay que adecuarla para mitigar los riesgos", incide.

Sin embargo, también señala que la compañía "ha mejorado la eficacia de los procedimientos" tomando acciones, correcciones, introduciendo cambios y refuerzo, lo que ha servido de "atenuante".

En el caso de Orange, la agencia publica dos sanciones, una de 70.000 euros y otra de 700.000 euros. La agencia ha tenido en cuenta denuncias como la de una cliente de Simyo al que le habían solicitado un préstamo de 43.000 tras el duplicado o la de un usuario de Orange al que le realizaron once transferencias en dos días por importe de hasta 5.000 euros.

En este contexto, la AEPD considera que también ha quedado probado que las medidas implantadas por Orange eran "insuficientes" y no sólo porque se haya producido su superación y la cesión de datos personales a un tercero. En su opinión, la superación por las personas suplantadoras de las políticas de seguridad implantadas por la operadora evidencia "un incumplimiento del deber de proteger la información de los clientes".

Aun así, también constató que, de la instrucción del procedimiento, se ha implementado "un modelo más eficaz de evitación del riesgo de suplantación de identidad", así como la revisión, el refuerzo y la mejora de las medidas de seguridad aplicadas en los distintos canales con el fin de evitar la materialización de los fraudes.

En lo que respecta a MásMóvil, se ha impuesto a la operadora una sanción de 200.000 euros tras tener en cuenta la investigación de oficio y dos reclamaciones de clientes que denuncian retiradas de dinero en cajeros o transferencias bancarias no autorizados.

El organismo considera que, a pesar disponer de unas medidas de seguridad que se deberían adoptar en los tratamientos de datos personales necesarios, estas han resultado "a todas luces insuficientes" para evitar el acceso indebido a duplicados de tarjeta SIM solicitados de forma fraudulenta.

07/02/2022. ¿Por qué considera Meta sacar Facebook e Instagram de la Unión Europea? FUENTE: elmundo.es

Mark Zuckerberg no está contento con la política de datos de la Unión Europea y, si nada cambia, podría bloquear el acceso a Facebook e Instagram en el continente. Es lo que deja entrever en uno de los informes que envía periódicamente a la SEC, la comisión que regula el mercado bursátil en Estados Unidos, donde explica que la política de la Unión en materia de protección de datos es inaceptable para la compañía.

La razón del descontento es una resolución preliminar de la Corte de Justicia Europea emitida en el mes de julio que considera que los servidores alojados en EE.UU. no operan bajo el marco de la GDPR, la ley de protección de datos personales.
Hasta ahora, y a pesar de las fuertes medidas de protección, empresas como Meta, Apple o Google podían seguir enviando datos de ciudadanos europeos a sus servidores centrales en Estados Unidos bajo el marco del conocido como Privacy Shield, un acuerdo firmado entre las dos regiones en 2016.

La nueva resolución, sin embargo, invalida este acuerdo al reconocer que las leyes de protección de datos son demasiado diferentes entre ambos mercados. Las medidas de protección que provee la GDPR sirven de poco si una vez en EE.UU. las empresas pueden hacer lo que quieren con esos datos de usuarios europeos o si el gobierno del país puede acceder a los mismos.

Aún es posible para las compañías extranjeras alojar datos de ciudadanos europeos en servidores situados fuera de la Unión, pero sólo si la UE ha certificado esas regiones como compatibles en materia de protección de datos personales. Nueva Zelanda, Japón, Suiza o Canadá son algunos de los países que cuentan con el visto bueno de la Unión en materia de datos.

El caso estadounidense es más complejo porque no hay una ley de datos federal que proteja la información de los usuarios con las mismas garantías que en la Unión Europea. Algunos estados, como California, tienen algunos mecanismos de protección parecidos que dan derecho a los usuarios a conocer qué información guardan las empresas sobre ellos y la opción de borrarlos.

"Si no se adopta un nuevo marco transatlántico de transferencia de datos y no podemos seguir confiando en otros medios alternativos de transferencia de datos de Europa a los Estados Unidos, es probable que no podamos ofrecer varios de nuestros productos y servicios más importantes, incluidos Facebook e Instagram, en Europa, lo que afectaría material y negativamente a nuestro negocio, condición financiera y resultados de las operaciones", ha explicado Meta en el comunicado a la SEC. La compañía espera que la Unión Europea emita una resolución definitiva sobre este asunto en la primera mitad de 2022.

En estos informes, elaborados también para los inversores, las compañías recopilan todas las posibles amenazas a su modelo de negocio, pero no son una guía estratégica y Meta podría optar, simplemente, por almacenar los datos de usuarios europeos en servidores locales y resignarse a una menor efectividad en sus herramientas publicitarias dado el mayor nivel de protección de los datos.

"No tenemos absolutamente ningún deseo ni planes de retirarnos de Europa, pero la simple realidad es que Meta, y muchas otras empresas, organizaciones y servicios, dependen de las transferencias de datos entre la UE y los Estados Unidos para operar servicios globales", explican desde la compañía.

La compañía, sin embargo, atraviesa un momento difícil. Tras la publicación de sus últimos resultados financieros ha perdido más de un cuarto de su valor en bolsa y parte de la razón es que cada vez le resulta más difícil explotar los datos de los usuarios para servir anuncios más relevantes. Sólo las medidas de protección de datos que Apple ha incluido en la última versión del sistema operativo de los iPhone, por ejemplo, le costará más de 10.000 millones de dólares en ingresos a lo largo de 2022.

12/02/2022 Se filtran los datos de 21 millones de usuarios a través de Telegram por utilizar VPN gratuitas. FUENTE: 20minutos.es

Muchos usuarios prefieren navegar a través de una VPN, ya que es una forma mucho más segura, puesto que se ocultan los datos de navegación a las páginas web que se hayan visitado.

Esta red privada virtual “falsifica” nuestra dirección IP original para que parezca que nos encontramos en una ciudad o hasta en un país distinto, es decir, se crea una red local sin que los integrantes estén físicamente en un espacio.

En caso de ser usuario de alguna de estas VPN gratuitas deberás tener cuidado, y es que 21 millones de usuarios han visto filtrados sus datos por haber hecho uso de este tipo de direcciones privadas. La filtración se habría producido en Telegram.

Muchos usuarios que querían navegar de una manera más segura, han acabado poniendo en peligro su información personal. Para entender como ha ocurrido esto hay que remontarse a 2021, donde en la DarkWeb se pusieron a la venta los datos de algunos usuarios

En ese momento no se supo quién los había comprado, pero ahora ya sabemos que son de dominio público y que con esta filtración, cualquier persona que tenga acceso a Telegram puede acceder a algunos datos como direcciones de correo electrónico, nombres de usuario, nombres de países o datos de facturación.

Esta información pertenece a más de veinte millones de personas que han visto filtradas sus contraseñas de acceso a sus cuentas de correo y además, los hackers también conocen los nombres de las personas que hay detrás.

El 99,5% de las direcciones de correo electrónico filtradas son cuentas de Gmail, un porcentaje bastante elevado que puede significar que no se compartió el volcado completo sino un subconjunto de datos.

Las aplicaciones gratuitas de VPN que habrían sufrido la filtración han sido GeckoVPN, SuperVPN y ChatVPN. Las tres habrían estado recopilando estos datos durante años y con su filtración, se ha puesto en peligro la seguridad de los usuarios.

Es muy difícil calcular de momento el impacto que va a causar aunque con estos datos en manos de los hackers, pero lo más probable es que comiencen una campaña de phishing para conseguir hacerse con la cuenta de cada persona y robar sus credenciales.

Los expertos recomiendan que en caso de haber utilizado alguna de estas VPN deberás proceder al cambio de contraseña de manera inmediata en tus cuentas de correo o en cualquier aplicación que consideres importante.

22/02/2022. ¿Pueden negarle a los padres el acceso a un informe médico de un hijo cuando ya es mayor de 14 años? FUENTE; diariosur.es

La historia clínica de un paciente recoge todos los datos, valoraciones e informaciones sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial, además de los médicos y demás profesionales que han intervenido en él. Su objetivo final es garantizar una asistencia adecuada, por eso, los profesionales que realizan el diagnóstico o el tratamiento, tienen acceso en todo momento a ese historial.

Pero además de los profesionales, ¿quién tiene derecho a ver la información que se recogen en ese informe médico? En ocasiones puede contener datos sensibles y los menores (caso de los adolescentes, por ejemplo) ver amenazada su intimidad si los profesionales revelan a sus padres datos de salud confidenciales. Pero, por otra parte, está el derecho de los padres a consultar la información sanitaria de sus hijos. Y es que contra este principio de reserva del secreto, está el interés legítimo del padre de ejercer la patria potestad como exige el Código Civil, para lo cual es imprescindible contar con la debida información sobre la salud de su hijo.

Así lo deja claro la Agencia Española de Protección de Datos (AEPD): «El artículo 154 del Código Civil habilitaría el acceso de los padres a la información sanitaria de sus hijos sobre los que ostenten la patria potestad para velar adecuadamente por su salud en cumplimiento de las obligaciones que impone el ejercicio de la patria potestad».

Sin embargo, el derecho de acceso al historial clínico solo se refiere a los titulares de la patria potestad, «no a cualquier familiar», zanjan.

Asimismo, cabe la posibilidad de que el menor de edad también pueda ejercer el derecho de acceso a su historia clínica a partir de los 14 años, «si bien este ejercicio no puede entenderse como limitación al derecho de los titulares de la patria potestad del menor no emancipado a acceder a su historia clínica».

Por último, en caso de reclamación por la negativa a entregar las historias clínicas de los menores a los padres que ostenten la patria potestad por querer proteger la intimidad del menor «deben dirigirse a las autoridades sanitarias o judiciales que correspondan», indican.

24/02/2022. El empresario responde por los medios puestos ante una violación de datos. FUENTE: eleconomista.es

La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultados sino de los medios empleados, según determina el Tribunal Supremo en sentencia de 15 de febrero de 2022.

Una vez que se produce una filtración de datos personales a un tercero no existe responsabilidad independiente de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento.

El ponente, el magistrado Córdoba Castroverde, razona que, en el supuesto examinado, el tribunal confirma la sanción a la empresa, de 40.000 euros, porque "el programa utilizado para la recogida de los datos de los clientes no contenía ninguna medida de seguridad que permitiese comprobar si la dirección de correo electrónico introducida era real o ficticia y si realmente pertenecía a la persona cuyos datos estaban siendo tratados y prestaba el consentimiento para ello.

Señala el ponente, que es cierto que los clientes afectados firmaron el formulario con la dirección de correo electrónico falsa, circunstancia que puede se ser tomada en consideración para graduar la sanción, pero que ni excluye la responsabilidad de la empresa ni puede encuadrase como una disminución sensible de su antijuricidad, a la que le sea aplicable el artículo 45.5 de la Ley Orgánica de Protección de Datos (LOPD), pues no puede considerarse que el cliente indujese a la comisión de la infracción, máxime cuando ese comportamiento y la dirección se ha reiterado en otros muchos clientes.

El estado de la técnica en el momento en el que se produjeron estos hechos permitía establecer medidas destinadas a comprobar la veracidad de la dirección de email, condicionando la continuación del proceso a que el usuario recibiese el contrato en la dirección proporcionada y solo desde ella prestase el consentimiento necesario para su recogida y tratamiento. Medidas que no se adoptaron en este caso".

Es decir, explica Córdoba Castroverde, que en el momento en que se produjeron estos hechos, existían medidas técnicas referidas al proceso de registro, que hubiesen evitado

la filtración de datos personales producida. Ello implica que las medidas técnicas adoptadas incumplían las condiciones de seguridad en los términos exigidos.

Por último, la Sala señala que el hecho de que fuese la actuación negligente de una empleada la que provocó la brecha de seguridad no le exime de responsabilidad a la empresa en cuanto encargada de la correcta utilización de las medidas de seguridad que deberían haber garantizado la adecuada utilización del sistema de registro de datos diseñado.

MARZO

01/03/2022. Protección de Datos multa a Amazon con dos millones de euros por exigir certificado de delito de penales para trabajar. FUENTE: eleconomista.es

La Agencia Española de Protección de Datos (AEPD) ha impuesto una multa de dos millones de euros a Amazon Road Transport Spain, filial de Amazon, por exigir el certificado de ausencia de penales como requisito para trabajar como repartidor en la compañía.

La idea de la denuncia surge de la demostración por parte de la Unión General de Trabajadores (UGT), de que Amazon Flex exigía a todos los candidatos que se presentaban al puesto de repartidor, de tener el certificado de penales como condición para formar parte del equipo.

La UGT señaló que la AEPD ha condenado a esta empresa por "vulnerar la intimidad de estas personas que si ya estaban obligados a trabajar como falsos autónomos además debían certificar que no contaban con antecedentes penales, una información sumamente personal que solo se puede solicitar cuando las empresas están facultadas legalmente para hacerlo y en el caso de cierto tipo de trabajos como el cuidado de menores".

"Tanto la Constitución como el Estatuto de los Trabajadores prohíben la discriminación de trabajadores y solicitar este tipo de certificados limitaría la posibilidad de la reinserción de quienes tienen antecedentes penales", añade UGT.

Por ello, el sindicato destacó que la AEPD ha calificado esta infracción como algo "muy grave". Además, ha tenido en cuenta la duración de la falta, resultando en un número de personas afectadas muy elevado. También, el nivel de daños provocados a las personas se ha visto afectado, ya que muchos no han podido acceder al trabajo y, para los que han accedido, se han expuesto a un riesgo ante su privacidad.

El sindicato consideró que "la negligencia apreciada en la comisión de la infracción, teniendo en cuenta que los requisitos exigidos por la entidad reclamada a los transportistas van más allá de lo requerido por la normativa reguladora del transporte de mercancías".

La UGT seguirá trabajando por el cumplimiento de los derechos, también sobre los de carácter personal y vigilando para que no se utilice la digitalización "como excusa para saltarse las normas y que las plataformas digitales no obliguen a facilitar datos para acumularlos, procesarlos e incluso para trabajar con ellos".

Pepe Álvarez, secretario general de la UGT, recordó que el modelo laboral de Amazon Flex ya fue sancionado anteriormente por la Inspección de Trabajo en octubre de 2020, por tener bajo su sistema de reparto a "falsos autónomos".

03/05/2022. Compartir contenidos de manera responsable a través de WhatsApp. FUENTE: aepd.es

Las aplicaciones de mensajería instantánea han evolucionado rápidamente y han ampliado sus funcionalidades más allá de los mensajes de texto. En la actualidad, aplicaciones como WhatsApp permiten compartir con otros usuarios o grupos audios, fotografías, vídeos, documentos o incluso nuestra ubicación en tiempo real.

La posibilidad de compartir audios, fotografías o vídeos desde nuestro teléfono móvil con un solo clic puede poner en riesgo nuestra privacidad y la de otras personas, por lo que debemos ser especialmente cuidadosos y usar la aplicación de manera responsable.

Falsa sensación de privacidad
El hecho de compartir estos contenidos a través de una aplicación de mensajería y no a través de una red social puede generarnos una falsa sensación de privacidad y de que mantenemos el control sobre la difusión de los mismos.

No obstante, una vez enviado cualquier contenido a través de WhatsApp u otras aplicaciones de mensajería, perdemos el control sobre el mismo. Igualmente ocurre si lo hacemos en un chat privado con otro usuario, ya que dependemos de la buena voluntad de esa persona para que la foto o vídeo no acabe reenviado en otros chats o grupos multitudinarios.

Puede suceder que un amigo o pareja que hoy consideramos de total confianza actúe de manera irresponsable o irreflexiva, o que, en el futuro, cambie su condición y utilice ese contenido para hacernos daño, como sucede en los casos de la llamada pornovenganza.

También debemos recordar que una imagen que consideramos inocente, divertida o sin importancia en un determinado momento de nuestra vida pueda llegar a avergonzarnos en un futuro o nos genere problemas en nuestro entorno social, familiar, afectivo o profesional.

Esta pérdida de control también afecta a los materiales audiovisuales que enviemos a través de la función de visualización única de WhatsApp, que elimina el contenido una vez visto. Recuerda que el destinatario puede guardar una copia para siempre haciendo una captura de pantalla o, por ejemplo, grabándola con otro móvil mientras el contenido se reproduce.

Contenido en el que aparecen otras personas
Todo lo comentado en este post es también aplicable al contenido que recibes a través de WhatsApp en el que aparecen otras personas. Si sospechas o es evidente que ha sido compartido sin consentimiento de las personas que aparecen, rompe la cadena. No lo reenvíes, ayuda a la víctima y acude a las autoridades si es preciso.

Conoce las herramientas de privacidad que te ofrece la app
En la web de WhatsApp encontrarás información detallada sobre todas las herramientas de control de privacidad que te ofrece la propia aplicación:

Controla la configuración de la privacidad en Android y iPhone.
Bloquea a usuarios no deseados en Android y iPhone.
Solicita información de tu cuenta.
Vacía los mensajes de un chat en Android y iPhone.
Desactiva las confirmaciones de lectura en Android y iPhone.
Elimina y reporta mensajes como spam.
Sal de un grupo en Android y iPhone.
Activa la verificación dos pasos.

Pide ayuda
Dependiendo de cada caso, además de utilizar las herramientas de bloqueo y reporte que te proporciona WhatsApp, puedes acudir a las autoridades o los servicios de ayuda de diferentes entidades y organizaciones:

Aplicación Alertcops de la Policía y la Guardia Civil

Policía Nacional

Guardia Civil

Unidad de Delitos Telemáticos de la Guardia Civil

Atención a víctimas de violencia de género 016

Instituto Nacional de Ciberseguridad INCIBE

Ayuda a niños, adolescentes, adultos y familias de la Fundación ANAR

Canal Joven de la AEPD

Recomendaciones básicas
Sigue estas recomendaciones básicas para compartir de manera responsable contenidos a través de WhatsApp:

Ten siempre presente que al pulsar el botón de enviar pierdes el control del contenido y dependes de la buena voluntad del quien lo recibe
Recuerda que la funcionalidad de visualización única no te garantiza que el destinatario no guarde una copia
No olvides que una foto o vídeo que hoy consideras inocente, inofensiva o divertida puede no parecértelo en un futuro y arrepentirte de su difusión
Considera el alto riesgo que suponen prácticas como el sexting o envío de contenidos íntimos de carácter sexual
No compartas contenidos en los que aparecen otras personas sin su consentimiento, puedes hacerles daño o incluso cometer un delito

Si recibes contenido sensible y sospechas o es obvio que está siendo difundido sin consentimiento de la víctima, rompe la cadena, reprocha esa conducta, ayuda a la víctima y acude a las autoridades.

Dispones de otros consejos sobre privacidad en WhatsApp en este post de nuestro blog y de información sobre cómo configurar las opciones de privacidad de Whatsapp en este vídeo del canal de YouTube de la Agencia.

04/03/2022 La AEPD multa a CaixaBank con 2 millones por ligar la exención de comisiones a la cesión de datos personales. FUENTE: europapress.es

La Agencia Española de Protección de Datos (AEPD) ha impuesto una sanción de más de 2 millones de euros a CaixaBank, como sucesora de Bankia, por una actuación llevada a cabo por la entidad ahora absorbida que vinculó la exención del cobro de comisiones de determinados productos a que los clientes diesen su consentimiento para recibir publicidad por cualquier canal habilitado y que sus datos personales pudiesen ser cedidos a otras empresas del grupo. Según recoge la AEPD en su resoluc ...

Leer más: https://www.europapress.es/economia/finanzas-00340/noticia-aepd-multa-caixabank-millones-ligar-exencion-comisiones-cesion-datos-personales-20220304135750.html

07/03/2022. La nueva Ley de Datos completa la estrategia europea. FUENTE: expansion.com

Nadie duda que los datos son la piedra angular de la transformación digital en el mundo, y particularmente en la Unión Europea, ya que afectan a todos los aspectos de la sociedad y de la economía y constituyen la base de nuevos productos o servicios.

Ya existen cuatro normas relevantes en el ámbito de los datos. El sobradamente conocido Reglamento General de Protección de Datos (RGPD) con su complemento, el Reglamento europeo para la libre circulación de datos no personales en la Unión Europea. La Directiva relativa a los datos abiertos, y el Reglamento europeo relativo a la protección de las personas físicas en el tratamiento de sus datos de carácter personal por parte de instituciones y organismos de la Unión Europea.

En este escenario, durante el año 2020, se publicó por parte de la Comisión Europea la Estrategia Europea de Datos con el fin de mejorar la eficiencia de un mercado único de datos. Uno de los principales pilares de la estrategia es el desarrollo de un marco de gobernanza intersectorial para el acceso conjunto a los datos entre entidades públicas y privadas.

Como consecuencia del desarrollo de la mencionada estrategia, nos encontramos en la tramitación de dos nuevas propuestas de reglamento muy relevantes y que tendrán consecuencias destacables. Por un lado, la propuesta de Reglamento europeo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) que tiene como finalidad que los datos fluyan libremente dentro de la UE y entre sectores para beneficiar a los ciudadanos, las empresas y las administraciones públicas. Y, por otro lado, la propuesta

de Reglamento europeo, publicada la semana pasada, que tiene por objeto armonizar el acceso equitativo a los datos por parte de las empresas y las instituciones (Ley de Datos).

Estas dos propuestas legislativas pretenden equilibrar el flujo y el uso de los datos, pero la pregunta es si este equilibrio, junto con la protección de la privacidad, la interoperabilidad y la ciberseguridad pueden suponer una desventaja competitiva para las empresas en el ámbito de la Unión Europea o en su propia posición frente a los competidores, ya que el tratamiento analítico de los datos (en este supuesto, no personales) de forma exclusiva ya es una ventaja competitiva en sí misma.

En cualquier caso, la citada Ley de Datos pretende garantizar que los usuarios de un producto o servicio (personas físicas o jurídicas) puedan acceder, de manera fácil, a los datos generados por el uso de dicho producto o servicio y que, además, dichos usuarios puedan utilizar los datos, incluso compartiéndolos con terceros de su elección.

La principal obligación para fabricantes de productos y proveedores de servicios que traten esos datos será diseñar y fabricar sus productos de tal manera que los datos generados por su uso sean, por defecto, fáciles, seguros y directamente accesibles para el usuario.

A partir de esa obligación será necesario informar, entre otras cuestiones, sobre la naturaleza, el volumen de datos, la forma de generación y el modo de acceder y compartir los datos. Cuando un "titular" de datos esté obligado a poner los datos a disposición de otro destinatario, debe hacerlo de manera interoperable y transparente, pero también puede obtener una compensación que se establecerá para cada caso concreto. Esto supone un avance en el debate sobre la monetización del uso de datos (sobre todo si esa compensación se traslada también a los usuarios).

La Ley de Datos intenta evitar los desequilibrios contractuales que dificulten el acceso y la utilización de forma equitativa de los datos para las pymes. La inclusión en un contrato de una cláusula contractual abusiva relativa al acceso a los datos y a su utilización no será vinculante para la pyme. Seguro que las características sobre la consideración de una cláusula como abusiva serán objeto de arduo debate hasta la versión definitiva del texto propuesto.

Este primer texto de la Ley de Datos también garantiza que los "titulares" de los datos (personas físicas o jurídicas que traten estos datos) los pongan a disposición de los organismos del sector público de los Estados miembros y de las instituciones, agencias u organismos de la Unión, cuando exista una necesidad excepcional y los datos necesarios para el desempeño de las tareas realizadas en interés público.

La configuración de la estrategia de datos europea va a propiciar un flujo de datos entre fabricantes, proveedores de servicios e instituciones de todos los sectores que, obviamente, ayudará a las empresas europeas a innovar y desarrollarse a nivel global. Sin embargo, las obligaciones derivadas del complejo mosaico regulatorio que se va configurando supone también una inversión en recursos que no será tarea fácil para ninguno de los interesados.

18/03/2022. Las reclamaciones presentadas ante la AEPD aumentaron un 35% en 2021. FUENTE: aepd.es

La Agencia Española de Protección de Datos (AEPD) ha publicado hoy su Memoria 2021, que recoge de forma exhaustiva las actividades realizadas, las cifras de gestión, los informes y procedimientos más relevantes del año, y un análisis de los retos presentes y futuros. La actividad de organismo en 2021 ha estado centrada de forma prioritaria en una doble vertiente: dar respuesta a los desafíos de protección de datos relacionados con la pandemia y seguir impulsando que aquellos que tratan datos se comprometan con la protección de la privacidad. En el primer bloque, la Agencia ha continuado participando en articular garantías para proteger los datos personales en los tratamientos relacionados con las medidas contra la COVID-19, tanto en un plano nacional como en el europeo a través del Comité Europeo de Protección de Datos (CEPD). En el segundo, en 2021 se puso en marcha el Pacto Digital para la Protección de las Personas, una iniciativa que ya cuenta con casi 400 entidades adheridas y que promueve la privacidad y la ética digital como un activo que las organizaciones deben tener en cuenta a la hora de diseñar sus políticas y sus estrategias.
En cuanto a las cifras de gestión, en 2021 se han presentado ante la Agencia 13.905 reclamaciones, un aumento de un 35% respecto a 2020. Esta cifra asciende a las 14.571 incluyendo los casos transfronterizos, los casos en los que la Agencia actúa por iniciativa propia y las quiebras de seguridad trasladadas a inspección. En 2021 las reclamaciones resueltas han aumentado un 35% (14.098) respecto al año anterior (10.443), una cifra muy destacable que ha permitido resolver reclamaciones pendientes de ejercicios anteriores sin que hayan aumentado significativamente los tiempos medios de resolución. En esos tiempos de tramitación de las reclamaciones hay que hacer una referencia a los traslados, una previsión recogida por la LOPDGDD para facilitar la resolución rápida de las reclamaciones y que ha permitido que estas se resuelvan en menos de dos meses.

Durante el año 2021 se ha seguido trabajando en el Canal Prioritario para solicitar la retirada urgente de contenido sexual o violento publicado en internet sin el permiso de las personas que aparecen en ellos. Así, se han recibido 377 peticiones a través del Canal Prioritario, de las cuales 215 han entrado a través del canal de menores. Se han realizado 25 intervenciones de urgencia después de determinar la naturaleza especialmente sensible de los datos personales divulgados y la afectación grave a la intimidad de las personas, consiguiendo la retirada de los contenidos sensibles con inmediatez.

En cuanto a las reclamaciones ordinarias, las planteadas con mayor frecuencia por los ciudadanos en 2021 corresponden a servicios de internet (16%), videovigilancia (12%), recepción de publicidad (excepto spam) (11%) e inserción indebida en ficheros de morosidad (9%). En cuanto a los procedimientos sancionadores, se finalizaron 585, un 49% más que en 2021. Las áreas más frecuentes en los procedimientos sancionadores son videovigilancia (25%), servicios de internet (22%), y publicidad a través de correo electrónico o teléfono móvil (9%).

Se han realizado 264 resoluciones que han finalizado con la imposición de multa. Las seis áreas de actividad con mayor importe global de multas han sido la publicidad (8.659.200 euros), telecomunicaciones (6.500.000 euros), entidades financieras/ acreedoras (6.243.000 euros), ficheros de morosidad (4.209.000 euros), contratación fraudulenta

(3.674.000 euros) y asuntos laborales (2.625.900 euros). Estas seis áreas suponen más del 90% del importe global de sanciones, que en 2021 ascendió a 35.074.800 euros. El incremento en la cifra de multas impuestas con respecto a años anteriores está relacionado con el mayor número de procedimientos sancionadores resueltos y también con la envergadura y complejidad de los casos, derivada de la magnitud de los tratamientos de datos investigados.

En cuanto a los casos transfronterizos, la Agencia ha iniciado 16 en 2021 y se ha declarado autoridad interesada en más de 300. Asimismo, se han recibido 1.070 peticiones de otras autoridades europeas, solicitudes de asistencia y consulta, y proyectos de decisión.

En lo referente a las sentencias de la Audiencia Nacional recaídas en los recursos interpuestos contra resoluciones de la Agencia, de las 66 dictadas en 2021, 56 (el 85%) fueron desestimatorias o inadmitidas. Por su parte, el Tribunal Supremo ha dictado 4 sentencias, todas ellas favorables a la Agencia.

En cuanto a las notificaciones de brechas de datos personales realizadas ante la Agencia, estas son inicialmente recibidas por la División de Innovación Tecnológica (DIT), que realiza un primer análisis. La DIT ha recibido y analizado 1.647 notificaciones en 2021, de las que poco más del 4% (76) se han remitido a la Subdirección de Inspección por requerir de una investigación en profundidad. Las brechas de datos personales más frecuentes son las causadas por ciberincidentes de origen externo/malintencionado y, dentro de este tipo de incidentes, el ransomware es el más repetido. En paralelo, siguen en aumento los casos en los que el cifrado de los datos y/o los sistemas van precedidos de una filtración de información y su puesta a la venta en internet/darkweb.

En lo relativo a las cifras de delegados de protección de datos (DPD) notificados ante la Agencia, 2021 se cerró con 82.249 DPD frente a los 65.040 DPD de 2020. De la cifra del año pasado, 74.033 corresponden al sector privado y 8.396 al sector público. Por lo que respecta a los servicios de ayuda que presta la Agencia para la adaptación al Reglamento, se han recibido casi 670 consultas a través del Canal del DPD, que da respuesta a las consultas que plantean los Delegados de Protección de Datos previamente notificados a la Agencia.

Por último, se han planteado casi 1.800 cuestiones ante el Canal Joven de la Agencia, un incremento de más del 28% respecto a 2020. Los progenitores han planteado el mayor número de consultas (54%) y, de forma agrupada, aglutinaron el 25% las cuestiones realizadas por responsables de empresas y organismos públicos que tratan datos de menores de edad, como clubs deportivos o entidades locales, o docentes de centros educativos.

21/03/2022. El Supremo suspende la renovación de la Agencia de Protección de Datos porque el proceso está "viciado de raíz". FUENTE; elpais.com

El Tribunal Supremo ha ordenado parar la renovación de la cúpula de la Agencia Española de Protección de Datos (AEPD) al considerar que el proceso iniciado en noviembre por el Gobierno "está viciado de raíz al apartarse de la normativa vigente". La decisión de la Sala de lo Contencioso-Administrativo responde a la petición de suspensión

cautelar de uno de los candidatos incluido en la terna para elegir al nuevo presidente de la AEPD, quien consideró que se había vulnerado su derecho fundamental al acceso a cargos púbicos en condiciones de igualdad "ante el hecho notorio de que el nombramiento estaba decidido antes de convocarse el proceso selectivo".

La cúpula de la AEPD, dirigida por Mar España, tenía que haberse renovado en 2019, pero la elección de la presidencia, que antes era discrecional del Gobierno, está regulada desde 2018 por una ley que exige una mayoría de tres quintos del Congreso. El PSOE y el PP incluyeron la agencia de protección de datos en el acuerdo que alcanzaron en octubre pasado para renovar el Tribunal Constitucional y el de Cuentas, y en el comunicado enviado a los medios la noche del 21 de octubre para comunicar los nombres de los elegidos para cada plaza, desvelaron que la AEPD pasaría a tener una presidenta, Belén Cardona –catedrática de Derecho del Trabajo y actual subsecretaria de Justicia, Interior y Administración Pública de la Generalitat valenciana–, propuesta por los socialistas, y una adjuntía a la presidencia, Borja Adsuara –abogado y consultor en derecho digital–, a iniciativa popular.

Pero la ley que regula desde 2018 la AEPD obliga a que su presidencia salga de una convocatoria pública, que no se había realizado cuando PSOE y PP comunicaron su acuerdo. Se convocó casi un mes después y concurrieron Cardona, Adsuara y otros 12 candidatos. Todos pasaron por un proceso de selección y, en febrero, el Consejo de Ministros, envió al Congreso una terna que propuso un comité de expertos para el puesto de presidente (que incluye a Cardona) y otra para el de la adjuntía (que incluye a Adsuara).

Los recursos presentados por dos de los candidatos también incluidos en las ternas se dirigen contra ese acuerdo del Consejo de Ministros. Uno de los recurrentes, Ricard Martínez, profesor de Derecho Constitucional de la Universidad de Valencia, había pedido al Supremo la suspensión cautelarísima (de urgencia y sin oír al resto de partes) del proceso, pero el tribunal lo rechazó el pasado viernes porque no hay evidencia de que el Congreso vaya a elegir de forma "inminente" al nuevo presidente. Pero los magistrados de la Sección Cuarta de la Sala de lo Contencioso sí aceptaron estudiar la suspensión cautelar solicitada por otro de los candidatos, Leonardo Cervera, director del Supervisor Europeo de Protección de Datos, y eso es lo que han acordado este lunes tras escuchar las opiniones de la Abogacía del Estado y de la Fiscalía, contrarias ambas a frenar el procedimiento.

El Supremo solo tenía que pronunciarse ahora sobre la paralización temporal del proceso, pero en el auto redactado para exponer su decisión dejan claras muestras de que, al menos su primera impresión, es que el Gobierno se ha saltado la normativa, "desde el momento en que, en puridad, no hay tal proceso, sino mera apariencia". La petición de suspensión cautelar tiene un fundamento "serio y atendible" porque el procedimiento está "viciado de raíz", advierte la sala, que señala dos supuestos incumplimientos. El primero, que los nombres de los futuros responsables de la Agencia fueron pactados por el Gobierno y el PP un mes antes de convocarse el proceso selectivo. El segundo, que la norma que regula este nombramiento establece que el Consejo de Ministros "debe remitir el nombre de un candidato para cada uno de los dos cargos al Congreso para su ratificación, pero no una terna por orden alfabético, como envió el Gobierno. "La consecuencia es que al apartarse del procedimiento, alterándolo de raíz, hasta el punto de transformar la fase de ratificación

parlamentaria por otra de elección, se ha actuado como si no existiese la vigente normativa y que, además, se ha procedido de modo que podría prestarse a dar cobertura formal a una designación ya hecha al hacerse la convocatoria", señalan los magistrados.

Para argumentar su decisión de suspender ahora el proceso, sin esperar a la sentencia que resolverá el fondo del asunto (si el procedimiento iniciado por el Gobierno es o no es legal), el Supremo sostiene que "el daño en término reputacional para la AEPD, dentro de España y ante la Unión Europea, sería mayor de dictarse una sentencia que declarase la nulidad del procedimiento de elección, con el consiguiente cese de unos cargos que son inamovibles".

24/03/2022. La AEPD impone una multa de 30.000€ a un hotel por incumplir el RGPD. FUENTE: hosteltur.com

La Agencia Española de Protección de datos impone una multa de 30.000€ a un establecimiento hotelero por lo que consideran una infracción del artículo 6 del RGPD, tipificada en el artículo 83.5.a) del RGPD y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPD. Pueden acceder a la Resolución en este enlace: https://www.aepd.es/es/documento/ps-00078-2021.pdf

La sanción viene motivada por una reclamación de carácter transfronterizo interpuesta ante la "Autoreit Persoonsgegevens", la autoridad de protección de datos de Países Bajos, contra el establecimiento hotelero por escanear el pasaporte de un cliente (incluida la fotografía) y utilizar dicha información personal para evitar un uso fraudulento de la tarjeta de consumo interno del hotel, comprobando y verificando la identidad del cliente al realizar cargos en la cuenta de su habitación con el objetivo de no causar un perjuicio económico a los clientes.

El hotel recogía y escaneaba los pasaporte de los clientes con la finalidad de cumplir con la normativa relativa al registro de entrada de viajeros en establecimientos de hostelería así como la obligación de comunicar la información contenida en las hojas-registro a las dependencias policiales, Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y la Orden INT/1922/2003, de 3 de julio,.

El problema surge cuando utilizan esa misma información que han recogido lícitamente en cumplimiento de una obligación legal (artículo 6.1. c) del RGPD), para una finalidad distinta sin el consentimiento del cliente.

Reacciones a la Resolución

Entre otros, la CEHAT o Confederación Española de Hoteles y Alojamientos Turísticos se han mostrado contrarios a esta resolución, ya que consideran que el escaneado del pasaporte de los turistas que pretenden alojarse en un hotel es un procedimiento habitual utilizado por los establecimientos o alojamientos turísticos para cumplir con las obligaciones legales de deber de información de registro de viajeros.

Entienden por este motivo, que es incoherente sancionar a un establecimiento hotelero por un acto supuestamente contrario al RGPD y a su vez exigible por el Ministerio del Interior.

Del mismo modo, les preocupa las exigencias contenidas en el Real Decreto 933/2021, de 26 de octubre, por el que se establecen las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor, solicitando que se retrase su entrada en vigor (próximo 28 de abril) ya que aún no existe un documento de desarrollo específico para los establecimientos hoteleros que se ajuste a los sistemas que utilizan.

Por otro lado, manifiestan la imposibilidad de recoger los datos solicitados en este Real Decreto ya que los establecimientos hoteleros no tienen acceso a los mismos o porque están prohibidos por normativa interna y comunitaria.

Esta normativa contempla al igual que el RGPD, importantes sanciones. Así mismo, exige a los hoteleros datos de las transacciones económicas a los que no tienen acceso por razones de seguridad, ya que son tratados por los proveedores de servicios de pago y plataformas que utilizan técnicas de encriptación siguiendo los protocolos aprobados por el Banco de España.

Aclaraciones de la Agencia Española de Protección de Datos

En este sentido, la Agencia Española de Protección de datos se ha pronunciado rápidamente al respecto dadas las reacciones, entre otras, de la Confederación Española de Hoteles y Alojamientos Turísticos (CEHAT), publicando ayer mismo un comunicado acerca del contenido de la resolución y la sanción impuesta al Hotel en relación al registro de datos de ciudadanos por parte de alojamientos turísticos: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-sobre-el-registro-de-datos-de-ciudadanos-por-parte

Las aclaraciones que realiza la AEPD se resumen en:

- Los alojamientos turísticos deben registrar datos de los documentos de identificación de sus clientes para cumplir las normas españolas sobre registros de viajeros y comunicarlos a las Fuerzas y Cuerpos de Seguridad del Estado en cumplimiento de la normativa de seguridad ciudadana.

- El establecimiento hotelero sancionado también recogía y utilizaba las fotografías de los clientes para el control de acceso y la facturación de sus consumos durante su estancia. No se incluía ningún detalle sobre la recogida y utilización de la fotografía, por lo que los clientes las desconocían. Tampoco se recogía este tratamiento en su Registro de Actividades de Tratamiento.

- La recogida y utilización de esas fotografías no están amparadas por las bases jurídicas de ejecución del contrato o cumplimiento de una obligación legal.

- La recogida y utilización de la fotografía supone un tratamiento de datos personales innecesario y desproporcionado para la finalidad establecida.

- Se ha requerido al establecimiento que cese en la recogida y tratamiento de la fotografía de sus clientes o, en caso contrario, adecúe la información en materia de protección de datos que ofrece a los clientes. Deben suprimir todas las fotografías recogidas de los clientes hasta el momento.

Conclusiones

Sea de nuestro agrado o no, la exigencia del cumplimiento del RGPD a las empresas se ha visto y se verá incrementada notablemente a medida que pase el tiempo.

Por ello, no debe extrañarnos que se produzcan de manera más frecuente este tipo de sanciones, por lo que se encuentra en mano de las empresas reforzar su protección en materia de seguridad de la información y cumplir con la norma de protección de datos personales.

Cumplimiento obligación legal. (art. 6.1.c RGPD) Deber de informar a las Fuerzas y Cuerpos de Seguridad del Estado en cumplimiento de la normativa de seguridad ciudadana

Es cierto que los establecimientos hoteleros deben cumplir con el deber de información sobre los datos de los viajeros para cumplir con la normativa de seguridad ciudadana y para ello recoger los datos identificativos del pasaporte, pero…

¿Realmente se necesita la fotografía del cliente para cumplir con el registro de viajeros?

Teóricamente, el proceso de escaneo al que se debería someter el pasaporte o documento identificativo de los clientes al realizar el check in, no consiste en obtener la imagen digital de todo el documento (escaneado común que todos conocemos), sino que se realiza utilizando un programa informático de reconocimiento óptico de caracteres (OCR) que identifica automáticamente los caracteres de un determinado alfabeto y los almacena en forma de datos, convirtiendo la imagen en texto.

De esta manera el establecimiento hotelero recaba los datos identificativos de sus clientes que posteriormente son remitidos a las Fuerzas y Cuerpos de Seguridad del Estado en cumplimiento de la normativa de seguridad ciudadana.

Uso de los datos personales del cliente para finalidad distinta. Falta de consentimiento (art. 6.1.a RGPD)

El problema en este caso radica en que se han utilizado los datos personales del cliente para otra finalidad distinta de la que había sido informada y de la que no se había obtenido su consentimiento. No es lícito recoger datos para finalidades distintas a las recogidas en el consentimiento del interesado o de las legalmente establecidas.

Para empezar, no se le informa al cliente en ningún momento de que se le va a recoger la fotografía del pasaporte para esa finalidad.

Por otro lado, tampoco consta en el registro de actividades del hotel, donde deben aparecer todos los procesos de tratamiento de datos personales, por lo que hasta el momento no hay ninguna base legal para utilizar ese dato como es la fotografía.

No se cumple con la minimización de datos (art. 5.1.c RGPD)

Por otro lado, parte de esa información personal que se había recogido, en este caso la fotografía, no era necesaria para la finalidad expuesta, por lo que tampoco se tiene en cuenta el principio de minimización de los datos. (artículo 5.1.c) RGPD). El objetivo de la minimización de datos es la de no excederse en la recogida de información, es decir, recopilar los datos mínimamente necesarios para la finalidad que se pretende.

Por otro lado, justifican la recogida de la fotografía, como veremos en el punto siguiente, en un interés legítimo que incumple de nuevo con la minimización de datos, ya que….

¿Realmente se necesita la fotografía del cliente para comprobar su identidad cuando se le hacen cargos a la tarjeta de consumo interno del hotel?

Hay muchísimas otras formas menos invasivas o intrusivas de comprobar si el titular de la tarjeta de consumo interno del hotel se corresponde realmente con el cliente, sin necesidad de conservar la fotografía del pasaporte.

Interés legítimo no justificado (art. 6.1.f RGPD)

En un primer momento, podemos pensar que estos hechos están justificados por el interés legítimo del artículo 6.1.f) del RGPD, como así hace constar el hotel entendiendo que existe un interés legítimo en cobrar al verdadero usuario del servicio evitando la utilización de las tarjetas de forma fraudulenta y que se carguen en las cuentas de los clientes, posibles consumos efectuados por terceros, es decir, que el fin justifica los medios.

Sin embargo, el mismo apartado del artículo dispone que “siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales…” que parece no haberse tenido en cuenta en este caso, ni haberse justificado, más aún, si cabe, cuando el propio interesado se negó a facilitar esa información.

En definitiva, consideramos que se pueden evitar estas sanciones y que se necesita mayor concienciación a nivel interno en las organizaciones para evitar este tipo de situaciones.

Por ello:

1- Solicita siempre el consentimiento del interesado para tratar sus datos personales e infórmale sobre la finalidad del tratamiento de sus datos.

2- Actualiza frecuentemente tu registro de actividades del tratamiento de datos personales y contempla en él todos los procesos.

28/03/2022. Nuevo acuerdo entre Europa y Estados Unidos por la transmisión y protección de datos. FUENTE: eleconomista.es

La Unión Europea (UE) ha anunciado un nuevo acuerdo con Estados Unidos (EEUU) sobre el flujo de datos transatlánticos que remplaza el fallido acuerdo del Escudo de la Privacidad en lo referido a la protección de datos de los usuarios.

El Escudo de la Privacidad era un acuerdo entre la UE y EEUU que marcaba la legislación en lo referido a la transmisión internacional de datos y en la consecuente protección de estos, sin embargo, en julio de 2020 el Tribunal de Justicia de la Unión Europea (TJUE) anuló este acuerdo declarando que no tenía un nivel adecuado de protección.

Desde entonces, se ha vivido en un marco de incertidumbre referido a la protección de datos, que ha causado múltiples problemas entre la UE y las grandes plataformas tecnológicas como Google o Facebook.

Ha sido durante una rueda de prensa conjunta de la presidenta de la Comisión Europea, Ursula Von der Leyen, y el presidente de los Estados Unidos, Joe Biden, en la que se ha anunciado este nuevo acuerdo transatlántico.

"Hemos encontrado un acuerdo de principio sobre un nuevo marco para los flujos de datos transatlánticos. Esto permitirá flujos de datos predecibles y confiables entre la UE y los EE. UU, salvaguardando la privacidad y las libertades civiles". Declaró Von der Leyen.

Hemos podido llegar a conocer algunos detalles de este nuevo acuerdo, gracias a un comunicado publicado por la Casa Blanca, en el que cabe destacar que se creará un mecanismo con varias capas en el que se incluye un Tribunal de Revisión de Protección de Datos independiente formado por personas elegidas fuera del gobierno estadounidense.

Aunque las críticas no han tardado en llegar, y es que los problemas con la protección de datos de los ciudadanos europeos se basan en la política de recopilación de EEUU, la cual ha causado que estos marcos legislativos hayan fracasado hasta en dos ocasiones anteriores. El activista y abogado especializado en privacidad, Max Shcrems ha sido uno de los primeros en postularse y ha augurado que esta nueva ley fracasará nuevamente debido al rechazo de EEUU de cambiar sus políticas.

No obstante, esta noticia también ha sido bien aceptada, en concreto por la industria tecnológica, que desde que se tumbó el Escudo de Privacidad han tenido que pelear para poder seguir operando y almacenando información de los usuarios europeos. Tendremos que esperar a ver cómo se desarrolla esta nueva normativa y sí la transmisión de datos entre la UE y EEUU cumple con los estándares de privacidad y seguridad necesarios.

ABRIL

18/04/2022. Brechas de datos personales: entornos de desarrollo y preproducción. FUENTE: aepd.es

Las grandes brechas de datos personales no siempre ocurren en los sistemas más importantes de una organización sino en sistemas secundarios que albergan una gran cantidad de información o pueden ser la puerta de entrada a otros sistemas. Este es el caso de los entornos de pruebas, preproducción o desarrollo, donde en ocasiones se realizan tratamientos de datos personales sin haber aplicado las medidas técnicas y organizativas adecuadas al riesgo para los derechos y libertades de los interesados, o que quedan olvidados y expuestos a Internet y acaban siendo la puerta de acceso a otros entornos con datos personales.

La ingeniería de sistemas establece la conveniencia de trabajar con varios entornos diferenciados: habitualmente, desarrollo, preproducción y producción. De forma general, lo recomendable es trabajar en el entorno de desarrollo, realizar las pruebas en el entorno de preproducción y finalmente desplegar aplicaciones y servicios en el entorno de producción. Desde la óptica de protección de datos, hay que tener en cuenta esta diferenciación y limitar la exposición de datos personales reales, y/o que estén en los sistemas de producción, en las fases de desarrollo y pruebas por el riesgo que puede suponer para los derechos y libertades de las personas.

Todavía es habitual encontrar entornos de desarrollo y preproducción en los que las medidas técnicas y organizativas orientadas a implementar las medidas y garantías establecidas en el Reglamento General de Protección de Datos (RGPD) se relajan, o que quedan expuestos a internet sin medidas de seguridad o abandonados y en desuso por lo que las medidas de seguridad pronto quedan obsoletas. Pero tampoco hay que olvidar que en algunos casos se empleen datos reales para pruebas de depuración de errores en labores de mantenimiento y/o desarrollo.

Con la aplicación del RGPD y la LOPDGDD, la situación respecto al uso de datos personales para pruebas en general, y en particular en entornos de desarrollo, se puede resumir brevemente a continuación.

En primer lugar, el RGPD en su artículo 32 Seguridad del tratamiento, establece que el responsable y el encargado de tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de los interesados. Luego el responsable y el encargado deben determinar las medidas de seguridad apropiadas con respecto al uso de datos personales reales en entornos de preproducción y pruebas. Además, deben establecer estas medidas teniendo en cuenta el nivel de riesgo específicamente con relación a la protección de datos, de igual forma que han de tener en cuenta los riesgos para la organización, como en cualquier entorno de producción.

En esta misma línea, el Supervisor Europeo de Protección de Datos (EDPS) en sus directrices “Guidelines on the protection of personal data in IT governance and IT management of EU institutions” indica:

80 En la fase de prueba, debe evitarse el muestreo de datos personales reales, ya que dichos datos no pueden utilizarse para fines para los que no fueron recogidos y su uso en entornos de prueba puede dar lugar a que personas no autorizadas dispongan de datos personales.

81 Siempre que sea posible, deben utilizarse datos de prueba creados artificialmente, o datos de prueba derivados de datos reales, de modo que se conserve su estructura pero no contengan datos personales reales. Diversas técnicas de este tipo se han aplicado con éxito.

82 Cuando un análisis minucioso y prudente muestra que los datos de prueba generados no pueden proporcionar suficiente garantía de la validez de las pruebas, debe tomarse una decisión exhaustiva y documentada, que defina qué datos reales se utilizarán en la prueba, lo más limitado como sea posible, las salvaguardias técnicas y organizativas adicionales que se establezcan en el entorno de las pruebas. Las categorías especiales de datos sólo pueden utilizarse en las pruebas de datos reales con el consentimiento explícito de las personas afectadas.

Y pone como ejemplo:

Ejemplo: en caso de errores en la operación del sistema, se debe evitar el uso de datos personales reales para la depuración del código. En cualquier caso, si es necesario, se debe obtener una autorización del responsable y tanto el proceso de autorización como las acciones de depuración deben registrarse y auditarse. De todos modos, se debe minimizar la cantidad de datos personales utilizados para las pruebas y se debe aplicar una política estricta de “need-to-know”.

Conforme al principio de minimización de datos y el principio de protección de datos desde el diseño y por defecto, cuando sea posible debe evitarse la utilización de datos personales en entornos de desarrollo y preproducción, o cualquier otro entorno de pruebas.

Además, las pruebas de software con datos personales son, o forman parte de, tratamientos de datos personales y el responsable del tratamiento debe cumplir con todas las obligaciones que se desprenden del RGPD.

Aunque no siempre es posible, en muchos casos la utilización de datos sintéticos evita el tratamiento de datos personales en pruebas de desarrollo. Existen servicios, algunos de ellos libres y de código abierto, para la generación de datos sintéticos de todo tipo bien conocidos en el sector.

Por tanto, cuando sea estrictamente necesario la utilización de datos personales en entornos de preproducción deberá documentarse mediante un análisis de necesidad y proporcionalidad, y en todo caso aplicar las medidas técnicas y organizativas que sean necesarias conforme al artículo 32 del RGPD y de acuerdo con el riesgo del tratamiento.

El riesgo en el entorno de preproducción podría ser el mismo que el riesgo del tratamiento en el entorno de producción. Pero también puede suceder que ese riesgo sea más elevado,

ya que es habitual contar con otros encargados de tratamiento en las labores de desarrollo, utilizar sistemas en la nube de proveedores diferentes a los entornos de producción, tener una mayor incertidumbre sobre la fiabilidad del código, llevar a cabo pruebas con nuevas tecnologías, etc. Por todo esto, los entornos de pruebas deberán de contar con medidas técnicas y organizativas de igual calado y, en todo caso, apropiadas para los riesgos específicos a la privacidad con independencia del contexto en el que fueran tratados, pues tal y como se señalaba por el grupo de trabajo del artículo 29, hoy Comité Europeo de Protección de Datos, en su declaración sobre el papel del enfoque de riesgos en el marco normativo de la protección de datos (WP218): "… Los interesados deben tener el mismo nivel de protección, independientemente del tamaño de la organización o la cantidad de datos que procesa. Por lo tanto, el Grupo de Trabajo considera que todos los responsables deben actuar de conformidad con la ley, aunque esto se puede hacer de manera escalable". Es decir, el contexto en el que tenga lugar un determinado tratamiento de datos no exime a los responsables de sus obligaciones a fin de proporcionar a los interesados el nivel de protección adecuado en cada caso con independencia de dicho contexto (desarrollo, preproducción o producción), y ello incluye el análisis de necesidad, proporcionalidad y de las bases jurídicas aplicables, además del resto de obligaciones exigidas en la normativa de protección de datos.

No aplicar la medidas técnicas y organizativas adecuadas al nivel de riesgo para los derechos y libertades en todos los entornos supone una vulneración del artículo 32 del RGPD e incluso puede suponer una vulneración de otros principios como los principios de finalidad, necesidad y proporcionalidad.

En relación con temas de brechas y datos personales puedes encontrar más material en la página de Innovación y Tecnología de la AEPD, en particular:

Brechas de seguridad: Ransomware y gestión del riesgo
Brechas de seguridad: el correo electrónico y las plataformas de productividad online
Brechas de seguridad: El Top 5 de las medidas técnicas que debes tener en cuenta
Brechas de seguridad: comunicación a los interesados
Brechas de seguridad: protégete ante la pérdida o robo de un dispositivo portátil
Brechas de seguridad de datos personales: qué son y cómo actuar
Brechas de seguridad: protégete ante el ransomware

17/04/2022. Diez preguntas claves sobre cómo adaptar los canales de denuncias al Anteproyecto de Ley del Gobierno. FUENTE: elconfilegal.com

Acaba de ser publicado el Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, elaborado por el Gobierno.

En este artículo vamos a definir los elementos claves que definen los canales de denuncia en el mencionado anteproyecto

1.- ¿NUEVOS TÉRMINOS?

El anteproyecto recoge una nueva nomenclatura para el conocido "Canal de denuncias" que adquiere la denominación de Sistema Interno de Información y el "denunciante" pasa a ser "informante".

2.- ¿CUÁLES SON LAS ENTIDADES PRIVADAS OBLIGADAS A IMPLEMENTAR EL SISTEMA INTERNO DE INFORMACIÓN?
El texto normativo habla de empresas de 50 o más trabajadores: se incluyen entidades que no tengan su domicilio en territorio nacional, pero desarrollen en España actividades a través de sucursales, agentes o mediante prestación de servicios sin establecimiento permanente.

También están obligadas los Partidos políticos y sindicatos, así como patronales y fundaciones creadas por los anteriores siempre que reciban o gestionen fondos públicos.

Junto a ellas empresas de menos de 50 trabajadores que implementen o tengan implementados canales éticos o de denuncias (por ejemplo, sujetos obligados en materia de prevención del blanqueo de capitales, empresas que tengan implementado un modelo de prevención de delitos, etcétera).

3.- ¿CÓMO FUNCIONA EN LOS GRUPOS DE EMPRESAS?
La sociedad dominante deberá aprobar una política general relativa al Sistema Interno de Información y se asegurará de que sea aplicado en todas las entidades que la integren, sin perjuicio de la autonomía de cada sociedad en relación con el respectivo sistema de gobierno corporativo y de las adaptaciones a la ley aplicable en cada caso.

Al mismo tiempo, el responsable del Sistema Interno de Información puede ser uno para todo el grupo o bien uno para cada sociedad integrante del mismo.

Es admisible el intercambio de información entre responsables del Sistema de un mismo grupo de empresas.

4.- ¿QUÉ DEBE HACER LA EMPRESA PARA CUMPLIR CON SU OBLIGACIÓN?
Se trata de implementar un Sistema Interno de Información que permita tramitar las comunicaciones que realicen los Informantes, previa consulta con la representación legal de las personas trabajadoras.

Al mismo tiempo, hay que nombrar al responsable del Sistema Interno de Información por parte del órgano de Administración. Si fuera nombrado un órgano colegiado, éste deberá delegar en uno de sus miembros las facultades de gestión del Sistema.

El siguiente paso es comunicar a la Autoridad Independiente de Protección del Informante (entidad pública que no existe por el momento) el nombramiento (y el cese cuando se dé) del responsable interno de Información.

Hay que decidir si la gestión del sistema se llevará internamente por el responsable del Sistema Interno de Información o bien se contratará a un gestor externo.

Es importante desarrollar un protocolo que regule el funcionamiento del Sistema Inferno de Información conforme a la legalidad vigente.

Hay además que comunicar y formar a los trabajadores sobre el Sistema Interno de Información

Comunicar externamente el Sistema Interno de Información. En caso de contar la empresa con página web debe publicarse en la página de inicio, en una sección separada y fácilmente identificable.

Es necesario contar con un libro-registro de las comunicaciones recibidas y de las investigaciones internas a que hayan dado lugar.

También es importante nombrar a un delegado de protección de datos (DPO) en caso de no disponer de uno. O incluir el tratamiento llevado a cabo en el Sistema Interno de Información dentro de las competencias del DPO existente en la entidad.

5.- ¿QUIÉN DEBE SER EL RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN?
Debe ser un alto directivo de la entidad que asuma exclusivamente dichas funciones y que ejerza su cargo con independencia del órgano de administración.

Cuando la naturaleza o dimensión de la entidad no justifique lo anterior, podrá ser desempeñado el cargo por persona que tenga otro cargo y funciones en la entidad.

En las entidades en que exista un responsable de Cumplimiento Normativo, entre los que se encuentra el «Compliance Officer», podrá ser ésta la persona designada.

6.- ¿QUIÉN PUEDE INFORMAR?
Informantes que trabajen en el sector privado y que hayan obtenido información sobre infracciones en un contexto laboral o profesional (trabajadores por cuenta ajena, autónomos, accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de la empresa, incluidos los miembros no ejecutivos).

Informantes que comuniquen información sobre infracciones obtenidas en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación, así como aquellos cuya relación laboral todavía no haya comenzado.

7.- ¿CÓMO DEBE SER EL SISTEMA INTERNO DE INFORMACIÓN?
Debe permitir la presentación de comunicaciones por escrito (correo postal, medio electrónico habilitado) y/o verbalmente (teléfono o sistema de mensajería de voz) y mediante reunión presencial. Las comunicaciones verbales deberán documentarse mediante grabación con consentimiento o transcripción escrita y firmada.

Al mismo tiempo debe permitir la presentación de comunicaciones anónimas e integrar los distintos canales internos de comunicación que existan en la empresa

Otra cuestión que debe es garantizar la confidencialidad de la identidad del informante, de las personas mencionadas en la comunicación y de las actuaciones que se desarrollen en la gestión y tramitación.

Al mismo tiempo debe cumplir con todas las previsiones en materia de Protección de Datos.

8.- ¿CUÁLES SON LOS PLAZOS ESTABLECIDOS?
En primer lugar, debe enviarse un acuse de recibo de la comunicación al informante en el plazo máximo de 7 días desde la recepción de la denuncia.

La investigación interna tiene un plazo máximo de tres meses desde la recepción de la comunicación, prorrogable otros tres meses en casos de especial complejidad.

Los datos personales relacionados con las comunicaciones y las investigaciones podrán conservarse un plazo máximo de 10 años.

9.- ¿QUÉ SUCEDE SI MI EMPRESA NO CUMPLE CON ESTA OBLIGACIÓN?
A la Autoridad Independiente de Protección del Informante se le atribuye potestad sancionadora. El Anteproyecto no establece la sanción aplicable al incumplimiento de la obligación de tener un canal de denuncias siendo sujeto obligado, pero sí regula sanciones a imponer a las empresas en caso de incumplir con las obligaciones que establece el anteproyecto para la gestión y tramitación de las denuncias.

Las sanciones previstas son:

Eso significa poder sufrir multas de hasta 1.000.000 euros en caso de infracciones muy graves.

Adicionalmente puede imponerse amonestación pública, prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo máximo de 4 años y la prohibición de contratar con el sector público durante un plazo máximo de tres años.

Publicación de las sanciones superiores a 600.000 euros en el Boletín Oficial del Estado.

10.- ¿QUÉ PLAZO TENGO PARA ADAPTARME A LA NORMATIVA?
Cuando se publique el texto legal definitivo las empresas dispondrán del plazo de 3 meses desde su entrada en vigor.

Para las empresas de menos de 249 trabajadores el plazo se extenderá hasta el 1 de enero de 2023.

20/04/2022. El Ayuntamiento de Estepona licita un sistema de cámaras inteligentes controladas por la Policía Local. FUENTE: malagahoy.es

El Ayuntamiento de Estepona informa que la ciudad contará con un novedoso sistema de cámaras que monitorizarán de forma inteligente el tráfico urbano y que reforzarán la seguridad en la ciudad. El Consistorio ha licitado este servicio con el objetivo de colocar

un total de 131 cámaras en 75 puntos del casco urbano y el extrarradio. Además, también se instalarán puntos de control en las zonas de acceso a Sierra Bermeja.

La centralización de la gestión del sistema se realizará desde el Centro de Control de la Jefatura de Policía Local aunque quedará también a disposición de otros Cuerpos de Seguridad que lo requieran. Con este nuevo dispositivo, el Consistorio tendrá capacidad para actuar con mayor celeridad en caso de que resulte necesario.

Otra de las novedades que aportará este sistema es que todos los vehículos patrulla de la Policía Local contarán con un dispositivo de asistencia técnica que les permitirá acceder a todas las videocámaras de tráfico instaladas en la vía pública. Todo esto contribuirá a que los policías reduzcan su tiempo de respuesta ante una intervención.

El teniente alcalde del área de Economía, Innovación y Recursos Humanos, José María Ayala, ha explicado que la instalación de sensores de inteligencia artificial también permitirá controlar las zonas de la ciudad donde existe gran afluencia. Así se contribuirá a minimizar el número de incidentes, atascos o delitos contra la seguridad vial en espacios con una importante actividad comercial, cultural o de ocio.

El nuevo sistema de cámaras inteligentes contempla también la instalación de una plataforma de sensores IOT que permitirán medir, entre otras cuestiones, datos metereológicos (temperatura, presión atmosférica, humedad relativa, lluvia, velocidad y direccionamiento del viento), calidad del aire y ruido, contribuyendo así a la disminución de la huella de carbono.

El responsable municipal de Economía e Innovación ha apuntado que este proyecto, que cumplirá con la legislación vigente en materia de seguridad y protección de datos personales, contempla también la instalación de un sistema de visualización y control de tráfico en tiempo real, mediante la colocación de un Centro de Procesamiento de Datos con conexión.

Este proyecto, que cuenta con un presupuesto de 500.000 euros (IVA incluido), incluido en la Estrategia de Desarrollo Urbano Sostenible e Integrable EDUSI ‘Estepona, Jardín de la Costa del Sol’, por lo que estará cofinanciada en un 80 por ciento por el Fondo Europeo de Desarrollo Regional (FEDER) de la Unión Europea. En este sentido, ha recodado que estas ayudas se enmarcan en el Programa Operativo de Crecimiento Sostenible (POCS) 2014-2020.

23/04/2022. Europa fija 3 nuevas técnicas que mejoran la protección de datos sanitarios. FUENTE: redaccionmedica.com

La seudonimización se está convirtiendo cada vez más en una técnica clave de seguridad de protección de datos y, además, ofrece "ciertas garantías sólidas para el resguardo de dichos datos personales, salvaguardando de esa manera los derechos y libertades de las personas". Así lo manifiesta en su último documento publicado la Agencia de la Unión Europea para la Ciberseguridad (Enisa, por sus siglas en inlgés). Este hecho es cada vez más frecuente sobre todo en el sector sanitario, ya que "este intenta aprovechar al máximo

la evolución de la tecnología y adecuar la prestación de sus servicios para atender de manera oportuna las crecientes necesidades de los pacientes".

Por ello, en el sector sanitario, "entran en juego los desafíos de ciberseguridad y la protección de los datos personales". Así, el organismo ha detallado en el documento tres nuevas técnicas sustanciales para mejorar la protección de dichos datos personales en el ámbito sanitario y son las siguientes:

Seudonimización determinista: usar siempre el mismo seudónimo para el mismo dato.
Documento de seudonimización aleatoria: utilizando el mismo seudónimo para los mismos datos solo dentro de un alcance consistente.
Seudonimización completamente aleatoria: siempre usando un seudónimo diferente para el mismo dato.

Estas nuevas técnicas son "sustanciales en cuanto a su implementación, ya que también es de suma importancia elegir la política con la que se aplicarán dichas técnicas", según el documento. En cuanto a las consideraciones de seudonimización, Enisa asegura que "los controladores y procesadores de datos en el ámbito sanitario pueden hacer uso de dichas técnicas ya sea de forma conjunta, usando siempre los mismos criterios, o inconexamente".

Valor añadido de la seudonimización en el ámbito sanitario

En un intento de demostrar el valor añadido de la seudonimización en el ámbito sanitario, Enisa presenta tres casos de uso en los que los datos médicos personales que se procesan son un seudónimo. En este sentido, el documento detalla que "si bien no se analizan en profundidad las técnicas específicas de seudonimización, los diferentes casos de uso intentan proporcionar una visión general de las posibilidades y de los aspectos clave de su aplicación". Todo ello con un único objetivo: " Aumentar el nivel de protección de los datos personales mediante la eliminación de identificadores personales directos". Estos tres casos son los siguientes:

Intercambio de datos de salud del paciente: en la práctica médica actual, el intercambio de datos entre organizaciones es una táctica común y se utiliza principalmente con fines diagnósticos y terapéuticos. Esto incluye los casos de intercambio entre diferentes departamentos dentro de la misma entidad, como un hospital, y entre individuos, como los profesionales médicos o laboratorios.
Ensayos clínicos: los ensayos clínicos estudian nuevas intervenciones y tratamientos médicos y evalúan sus efectos directos y los posibles efectos secundarios. Se considera un requisito previo para adquirir la aprobación necesaria de las autoridades pertinentes. Por ello, y en general, no los realiza el fabricante, sino organizaciones independientes denominadas Organizaciones de Investigación Clínica (CROs, por sus siglas en inglés).
Monitoreo de datos de salud orientados al paciente: actualmente, los dispositivos portátiles inteligentes pueden controlar los signos vitales, como la frecuencia cardíaca, el nivel de oxígeno o de presión arterial, entre otros. El control regular de dichos signos es una intervención común en el cuidado del paciente que tiene como objetivo facilitar el reconocimiento temprano de las alteraciones fisiológicas. Sin embargo, solo el propio

paciente debería ser quien pueda visualizar las mediaciones y ponerse en contacto con su médico cuando se observe un valor anormal.

Cabe señalar que estos casos de uso sirven "para demostrar la aplicación de seudonimización y no intentar cubrir los casos de uso operativos en toda su extensión, es decir, que los procesadores de datos deberían de tener en cuenta todas las operaciones de tratamiento de datos pertinentes".

Los diferentes avances en la tecnología y en los tipos de servicios relacionados con la salud "pueden afectar en la eficacia y aplicabilidad de la seudonimización que a día de hoy ya se está implantando". Esto, según Enisa, "no solo es relevante para la elección de las técnicas utilizadas, sino también para el diseño general de proceso de seudonimización incluyendo la protección de la información adicional, como es la información que permite asociar los seudónimos con los identificadores iniciales".

Enisa también alerta de "los desafíos o limitaciones de implementación que pueden surgir con respecto a cada una de las nuevas técnicas presentadas". Por ello, el organimso europeo anima a que "la comunidad investigadora sigua trabajando en la protección y seguridad de los datos, incluidas las técnicas de seudonimización de última generación y sus posibles implementaciones, con el apoyo de las instituciones de la Unión Europea en términos de orientación política y fondos de investigación", concluye.

MAYO

04/05/2022. Nueva sección sobre salud y protección de datos. FUENTE: aepd.es

La Agencia Española de Protección de Datos (AEPD) ha publicado en su sección Áreas de interés un nuevo espacio web que facilita la consulta y sistematiza la información sobre el tratamiento de datos de salud, un área de actuación prioritaria para la AEPD. El objetivo de esta área es dar respuesta al planteamiento manifestado por representantes del sector sanitario y asociaciones de usuarios de contar con un compendio de legislación, criterios, doctrina y precedentes en materia de salud y protección de datos.

Los datos personales relativos a la salud están considerados como una categoría especial y, por tanto, especialmente protegidos. En 2021 se registraron 680 reclamaciones relacionadas con sanidad, incrementándose un 75% respecto a 2020.

Los contenidos de la sección están destinados a ciudadanos, responsables de tratamientos, profesionales de la protección de datos, centros sanitarios o la industria farmacéutica, entre otros.

La nueva sección está compuesta por siete apartados que recogen desde información general sobre el tratamiento de los datos de salud y cómo ejercer el derecho de acceso a la historia clínica hasta cuestiones relacionadas con la investigación médica. También recoge los criterios marcados por la Agencia a partir de consultas planteadas por el sector sanitario, además de información sobre expedientes e inspecciones de oficio realizadas.

Entre las novedades incluidas en este nuevo apartado se encuentran los temas relacionados con la investigación sanitaria y los ensayos clínicos, así como las brechas de datos personales en el sector de la salud. En el segundo semestre de 2021, el 15% de las notificaciones de brechas recibidas en la Agencia las realizaron responsables del tratamiento cuyo sector de actividad principal es el asistencial en el ámbito de la salud.

05/5/2022. La AN ratifica la sanción de la AEPD de 250.000 euros a LaLiga por el uso de su 'app' móvil. FUENTE: confiegal.com

La Audiencia Nacional (AN) ha ratificado la resolución de la Agencia Española de Protección de Datos (AEPD), de 10 de junio de 2019, y la sanción de 250.000 euros a LaLiga de Fútbol Profesional por el uso de su aplicación móvil.

La sentencia, que se ha hecho pública esta semana, fue dictada el 11 de octubre de 2021 por el tribunal de la Sala de lo Contencioso-Administrativo (Sección Primera), con ponencia del presidente de dicha Sección, el magistrado Eduardo Menéndez.

Esta sentencia confirma el fallo del regulador y subraya la infracción del artículo 5.1.a) del 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 y por el que se deroga la Directiva 95/46/CE (RGPD).

Como ya adelantase en su día Confilegal, LaLiga decidió acudir a la vía judicial tras la resolución de la AEPD que imponía dicha multa por una supuesta infracción del principio de transparencia a la hora de informar en la 'app' oficial sobre el uso de la funcionalidad del micrófono en el momento de su activación.

Desde La Liga se discrepó profundamente de esta decisión, rechazando la sanción impuesta por injusta, y considerando que la AEPD no ha realizado el esfuerzo necesario para entender cómo funciona la tecnología.

Ahora, en esta resolución que la Audiencia Nacional acaba de dar a conocer, la Sala de lo Contencioso mantiene las tesis del regulador de protección de datos y confirma la infracción y la multa. Solo le quedaría a LaLiga un posible recurso de casación ante el Tribunal Supremo.

Javier N. Seoane, abogado experto en Derecho Público y en nuevas tecnologías, hace un análisis de este relevante fallo judicial: "Como puede deducirse, la Audiencia Nacional sigue las tesis de la AEPD y ofrece una interpretación muy protectora de la privacidad. Lo avala completamente".

Este jurista recuerda que en junio de 2019 la AEPD impuso a LaLiga de Fútbol Profesional una multa de 250.000 euros y la exigencia de adecuación de la aplicación móvil por tratamiento ilícito de datos personales derivado de ciertas funcionalidades de la 'app' LaLiga.

"Una aplicación que geolocalizaba y espiaba el sonido ambiente", aclara este experto en privacidad.

De hecho, destaca que entre tales funcionalidades "se activaba -sin permiso específico del usuario- la grabación del sonido ambiente, donde se llegaban a grabar conversaciones que incluyan datos personales, entre otros sonidos.

También queda probado en dicho fallo que la aplicación gestionaba otros datos personales a nivel de grabar como puede ser los de la dirección IP; identificadores ad hoc; huellas digitales como hacen otras aplicaciones».

NECESIDAD DE PERMISO ESPECÍFICO

Para Seoane, la propia resolución de la Audiencia Nacional confirma la exigencia de la AEPD de que "no basta con un permiso genérico cuando te descargas la 'app', lo que se viene a exigir por parte del regulador es que cada vez que se activase el micrófono, el usuario tuviera un aviso o alguna señal que le advirtiera que se estaba utilizando ese micro para esos fines".

También recuerda que la AEPD había sido muy rigurosa en la fundamentación de la sanción al no considerar como anonimización irreversible el riesgo Indirecto de identificación del usuario (transformación de archivo de audio y creación de identificador ad hoc).

Tras descartar varias infracciones en el procedimiento sancionador, la sentencia de la Audiencia Nacional concluye que la interpretación de la AEPD del requisito de transparencia es razonable porque no se entiende que la 'app' avise cada que vez que se activa la geolocalización, "pero no cuando se activa el micro".

Al mismo tiempo, la resolución señala que la finalidad de la 'app', como es de colaborar en la lucha contra la piratería, sobre todo de locales de hostelería que emiten los partidos sin licencia, exige que haya más transparencia en el uso de esa aplicación,

Para este jurista, "si no se descarta por el Tribunal Supremo, cuando se descargue esta 'app' o una similar, tiene derecho a un aviso cada vez que se active el micro y en ese momento poder revocar el consentimiento». Se trata de que el usuario sepa cuando se utiliza ese micro para tener capacidad para revocarlo si se quisiera hacer".

En el fundamento sexto de la sentencia se indica que «el tratamiento de datos debe ser objeto de una información clara, fácil de acceder e inteligible para el titular de los datos, facilitando que su consentimiento sea correctamente informado y posibilitando el ejercicio de sus derechos».

La resolución considera que «el tratamiento de datos que se realiza a través de la aplicación de LaLiga en los dispositivos móviles de los usuarios, derivado de la funcionalidad del micrófono, vulnera el principio de transparencia ya que presta inicialmente su consentimiento al instalar la aplicación, pero ignora el momento en que ésta recoge sonidos a través del micrófono en cada ocasión en que se activa, que es cuando se produce el tratamiento y cuando es de utilidad para LaLiga".

PROTECCIÓN DE LA PRIVACIDAD

Esta jurista cree que "este es un concepto de la transparencia muy evolucionado y muy protector de la privacidad y de los datos personales que no se había llegado tan lejos en este punto en concreto".

Sobre los argumentos que ofrece esta sentencia son dos demoledores para este jurista, "uno, en cuanto a la activación del audio viene a decir, con toda lógica, que si hay un aviso cuando se activa la geolocalización, como no se va a avisar cuando se activa el micrófono para grabar el sonido ambiente. No tiene lógica que no se haga así, en este caso".

Y el segundo argumento, "de más calado todavía, tiene que ver con que si estas utilizando a un usuario a través de una aplicación como colaborador para la lucha contra la piratería, lo lógico es que haya la máxima transparencia y tenga derecho a conocer cuando está siendo grabando, que es lo que tiene derecho a conocer cada usuario".

En esta resolución, la propia Audiencia Nacional ratifica también el importe de la sanción que también se había cuestionado. "Ese importe se calcula como dice la ley en materia de protección de datos. Es en función del volumen de facturación que tienen la propia Liga de Fútbol Profesional con esa aplicación, es un porcentaje sobre eso y no hay nada que discutir".

Javier Seoane recuerda que esta sanción tiene su origen en el 2019," ahora hay algunas aplicaciones que han mejorado en ese sentido y te piden un permiso específico para activar geolocalizaciones o notificaciones de este tipo. Hasta la fecha el aviso son unos puntos rojos que se ven en los Iphone. Es el momento que una aplicación quiere acceder a tu cámara o al micro

Para este experto, "no tiene que ser Apple la que avise, sino que debería ser la propia aplicación la que avisara sobre esta cuestión, así lo señala la AEPD en este fallo en el que pide a LaLiga que ese micro avise siempre que vaya actuar para que el usuario sepa que le pueden estar grabando. Eso es algo que quiere la AEPD que tengan todas las aplicaciones".

Desde su punto de vista, un fallo de este tipo puede entenderse en que frena la innovación y el desarrollo de las aplicaciones, "pero no se puede olvidar que la privacidad es un derecho fundamental que debe tener su protección específica".

Seone recuerda que en su momento, cuando se dio a conocer la resolución de la AEPD, en junio del 2019, algunos expertos indicaron que se había ido demasiado lejos. Sin embargo, ahora la Audiencia Nacional confirma, con este fallo, la exigencia de transparencia.

"Se ve que nuestro regulador de privacidad está alineada con el resto autoridades de protección de datos europeos. Estamos hablando de una interpretación del RGPD Europeo "según dice la sentencia muy razonable y protectora de la privacidad y de los datos personales", finaliza.

06/05/2022 Más de 40 detenidos en una trama de robos de datos personales a una empresa eléctrica. FUENTE; rtve.es

La Policía Nacional ha detenido a 44 personas en 12 provincias españolas en una trama de empresas que robaban presuntamente datos personales de clientes de una empresa eléctrica para derivarlos a una compañía de la competencia y enriquecerse de las comisiones por la captación de nuevos clientes.

La operación Nikola se ha saldado con 44 arrestos en Barcelona, Cádiz, Castellón, Ciudad Real, Córdoba, Huelva, Jaén, Madrid, Málaga, Murcia, Sevilla y Valencia por un delito contra el mercado y los consumidores, ha informado la Dirección General de la Policía. De los detenidos, 26 eran comerciales, a los que también se les imputa un delito de usurpación de estado civil, y 18 eran administradores de una sociedad denominada 'Fuerza de ventas', cuya función era captar lícitamente a clientes para la eléctrica que la tenía subcontratada.

Sin embargo, esta sociedad investigada contrató a su vez a nuevas empresas para aumentar el tráfico de datos personales que se convertían en nuevos clientes de la eléctrica, que no conocía la existencia de estas prácticas ilegales.

Los investigadores comprobaron que los implicados en el fraude, trabajadores y administradores de estas empresas, estaban cobrando parte de la comisión que recibía la sociedad 'Fuerza de ventas' por la captación de nuevos clientes.

Unos 36.000 cambios de datos
Se estima que los investigados realizaron unos 36.000 cambios de datos confidenciales que han causado baja en la empresa eléctrica perjudicada, habiéndose informado de estos hechos a la Dirección de Competencia de la Comisión Nacional del Mercado de Valores (CNMV). También se comunicaron a la Agencia Española de Protección de Datos por si el robo acometido pudiera ser susceptible de sanciones.

La investigación policial se inició en septiembre de 2019 a raíz de una denuncia interpuesta por el administrador de una compañía eléctrica, en la que manifestaba que personas desconocidas se hacían pasar por trabajadores de la empresa y estaban llamando a sus clientes. Estos 'call centers' conocían todos sus datos personales, bancarios y puntos de suministro, y les ofrecían un supuesto descuento en la tarifa, cuando en realidad los cambiaban a otra compañía eléctrica sin su conocimiento.

La empresa denunciante realizó una auditoría interna en la que detectaron que se habían producido accesos no autorizados a sus bases de datos. Además, supieron que personas desconocidas habían contactado con la compañía haciéndose pasar por sus clientes y, tras contestar las preguntas de seguridad, solicitaban duplicados de facturas a fin de comunicar un cambio en sus datos personales.

Los investigados lo hacían para evitar que, al verdadero cliente, que desconocía su nueva alta en otra empresa eléctrica, le llegase una posible contraoferta de la compañía afectada. En paralelo, la eléctrica que recibía los nuevos clientes interpuso una querella contra varios comerciales de su sociedad 'Fuerza de ventas' al conocer estas prácticas.

Una vez atada la investigación e identificados los implicados en la trama, la Policía llevó a cabo un operativo en tres fases en las que se llevaron a cabo la totalidad de las detenciones.

18/05/2022. La AEPD sanciona a Google LLC por ceder datos a terceros sin legitimación y obstaculizar el derecho de supresión. FUENTE: aepd.es

La Agencia Española de Protección de Datos (AEPD) ha dictado resolución del procedimiento iniciado contra la compañía Google LLC en la que declara la existencia de dos infracciones muy graves de la normativa de protección de datos e impone una sanción de 10 millones de euros por ceder datos a terceros sin legitimación para ello y obstaculizar el derecho de supresión de los ciudadanos (artículos 6 y 17 del Reglamento General de Protección de Datos).

Google LLC es la responsable del tratamiento analizado y lo lleva a cabo en EEUU. En el caso de la comunicación de datos a terceros, la Agencia ha constatado que Google LLC envía al Proyecto Lumen información de solicitudes que le realizan los ciudadanos, incluida su identificación, dirección de correo electrónico, los motivos alegados y la URL reclamada. La misión de ese proyecto es la recogida y puesta a disposición de solicitudes de retirada de contenido, por lo que la Agencia considera que, dado que se remite toda la información contenida en la solicitud del ciudadano para que se incluya en otra base de datos accesible al público y para que se divulgue a través de una web, "supone en la práctica frustrar la finalidad del ejercicio del derecho de supresión".

La resolución recoge que esta comunicación de datos por parte de Google LLC al Proyecto Lumen se impone al usuario que pretenda utilizar sus formularios, sin opción de oponerse a la misma y, por tanto, sin que exista un consentimiento válido para que esa comunicación se lleve a cabo. Establecer esta condición en el ejercicio de un derecho reconocido a los interesados no está amparado por el Reglamento General de Protección de Datos al generarse "un tratamiento adicional de los datos sobre los que versa la solicitud de supresión al comunicarlos a un tercero". Además, en la política de privacidad de Google LLC, no se hace mención a este tratamiento de datos personales de los usuarios, y tampoco aparece entre las finalidades la comunicación al Proyecto Lumen.

La AEPD también recoge en su resolución que, presentada la solicitud de retirada de contenido y atendido el derecho, es decir, acordada la supresión de los datos personales, "no cabe un tratamiento posterior de los mismos, como es la comunicación que Google LLC realiza al Proyecto Lumen".

En cuanto al ejercicio de derechos de los ciudadanos, la AEPD detalla en su resolución que "es difícil deducir si la solicitud se formula invocando la normativa de protección de datos personales, sencillamente porque esta normativa no se menciona en ninguno de los formularios, con independencia del motivo que el interesado seleccione de entre las opciones propuestas, salvo en el formulario denominado 'Retirada en virtud de la ley de privacidad de la UE', el único disponible que contiene una referencia expresa a esta normativa".

El sistema diseñado por Google LLC, que conduce al interesado a través de diversas páginas para llegar a cumplimentar su solicitud, obligándole previamente a marcar las opciones que se ofrecen, "puede provocar que este termine marcando una opción que se adapte a los motivos que considera apropiados a su interés, pero que le aparta de su intención originaria, que puede estar claramente vinculada a la protección de sus datos personales, desconociendo que estas opciones le sitúan en un régimen normativo distinto porque así lo ha querido Google LLC o que su solicitud se resolverá según las políticas internas establecidas por esta entidad". La resolución de la Agencia recoge que este sistema es un equivalente a "dejar a criterio de Google LLC la decisión sobre cuándo aplica y cuándo no el RGPD, y esto supondría aceptar que esta entidad pueda eludir la aplicación de la normativa de protección de datos personales y, más concretamente para este caso, aceptar que el derecho de supresión de datos personales quede condicionado por el sistema de eliminación de contenidos diseñado por la entidad responsable".

Adicionalmente a la sanción económica impuesta en la resolución, la Agencia también ha requerido a Google LLC para que adecúe a la normativa de protección de datos personales la comunicación de datos al Proyecto Lumen, y los procesos de ejercicio y atención del derecho de supresión, en relación con las solicitudes de retirada de contenido de sus productos y servicios, así como la información que ofrece a sus usuarios. Asimismo, Google LLC deberá suprimir todos los datos personales que hayan sido objeto de una solicitud del derecho de supresión comunicada al Proyecto Lumen, y tiene la obligación de instar a este último para que suprima y cese en la utilización de los datos personales que le haya comunicado.

18/05/2022. El Consejo aprueba la Ley de Gobernanza de Datos. FUENTE: cde.ual.es

Tras el Parlamento Europeo, el Consejo ha aprobado el 16 de mayo una nueva ley para promover la disponibilidad de los datos y construir un entorno fiable que facilite su uso para la investigación y la creación de nuevos servicios y productos innovadores.

La Ley de Gobernanza de Datos (DGA) establecerá mecanismos sólidos para facilitar la reutilización de determinadas categorías de datos protegidos del sector público, aumentar la confianza en los servicios de intermediación de datos y fomentar el altruismo de datos en toda la UE.

Se trata de un componente importante de la estrategia europea para los datos, cuyo objetivo es impulsar la economía de los datos. Las nuevas normas se aplicarán 15 meses después de la entrada en vigor del Reglamento.

Reutilización más amplia de los datos protegidos del sector público
La Ley de Gobernanza de Datos creará un mecanismo para permitir la reutilización segura de determinadas categorías de datos del sector público que están sujetos a los derechos de terceros. Esto incluye, por ejemplo, secretos comerciales, datos personales y datos protegidos por derechos de propiedad intelectual. Los organismos del sector público que permitan este tipo de reutilización deberán estar debidamente equipados, en términos técnicos, para garantizar la plena preservación de la privacidad y la confidencialidad.

En este sentido, la DGA complementará la Directiva de Datos Abiertos de 2019, que no cubre este tipo de datos.

Los acuerdos exclusivos para la reutilización de datos del sector público serán posibles cuando estén justificados y sean necesarios para la prestación de un servicio de interés general. La duración máxima de los contratos existentes será de 30 meses y la de los nuevos de 12 meses.

La Comisión creará un punto de acceso único europeo con un registro electrónico de datos del sector público que permita realizar búsquedas. Este registro estará disponible a través de las ventanillas únicas nacionales.

Un nuevo modelo de negocio para la intermediación de datos
La DGA crea un marco para fomentar un nuevo modelo de negocio -servicios de intermediación de datos- que proporcionará un entorno seguro en el que las empresas o los particulares podrán compartir datos.

En el caso de las empresas, estos servicios pueden adoptar la forma de plataformas digitales, que apoyarán la puesta en común voluntaria de datos entre empresas y facilitarán el cumplimiento de las obligaciones de puesta en común de datos establecidas no sólo por esta ley, sino también por otra legislación, ya sea a nivel europeo o nacional. Mediante el uso de estos servicios, las empresas podrán compartir sus datos sin temor a que se haga un uso indebido de ellos o a perder su ventaja competitiva.

En el caso de los datos personales, estos servicios y sus proveedores ayudarán a las personas a ejercer sus derechos en virtud del Reglamento General de Protección de Datos (RGPD). Esto ayudará a las personas a tener un control total sobre sus datos y les permitirá compartirlos con una empresa en la que confíen. Esto puede hacerse, por ejemplo, mediante novedosas herramientas de gestión de la información personal, como los espacios de datos personales o las carteras de datos, que son aplicaciones que comparten esos datos con otros, basándose en el consentimiento del titular de los datos.

Consejo Europeo de Innovación de Datos
Se creará una nueva estructura, el Consejo Europeo de Innovación de Datos, para asesorar y asistir a la Comisión en la mejora de la interoperabilidad de los servicios de intermediación de datos y emitir directrices sobre cómo facilitar el desarrollo de los espacios de datos, entre otras tareas.

JUNIO

17.06.2022. La protección de datos del estudiante en prácticas. FUENTE. Blogs.elconfidencial.com

Es un tema recurrente a la hora de elaborar los convenios de prácticas entre las universidades y las empresas u otro tipo de entidades a las que los alumnos vayan a acudir a realizar sus prácticas, el de determinar la posición de las dos partes en relación con los datos personales de los alumnos. Del 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos - RGPD), se derivan distintas posibilidades.

Una sería la corresponsabilidad regulada en el artículo 26: "1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento […]". Sin embargo, en el caso de las prácticas universitarias existen obligaciones de las universidades y las entidades colaboradoras que no son comunes y, por tanto, difícilmente pueden determinar conjuntamente los fines y medios de algunos de los tratamientos que han de realizar en relación con los datos personales de los alumnos.

Por poner solo un par de ejemplos, si las prácticas son remuneradas por la empresa, esta tendrá la obligación de dar de alta a los alumnos en la Seguridad Social y ahí difícilmente tendrá algo que decidir la universidad. Lo mismo si la entidad en la que el alumno está haciendo sus prácticas es un hospital: los datos identificativos del alumno podrán acabar figurando en la historia clínica del paciente y, de nuevo, será únicamente el hospital quien decida los objetivos y medios de ese tratamiento. No habrá una determinación conjunta por parte del hospital y la universidad a este respecto.

Algo similar ocurre con la posibilidad de entender que la universidad es responsable del tratamiento y la empresa solo una encargada del tratamiento, conforme a lo dispuesto en el artículo 28 RGPD: "1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes […].

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico […]. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, […];

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros; […]".

Las prácticas universitarias están reguladas fundamentalmente en el Real Decreto 592/2014, de 11 de julio, por el que se regulan las prácticas académicas externas de los estudiantes universitarios. Es este Real Decreto el que establece las obligaciones que han de cumplir las universidades y las entidades colaboradoras, detallando incluso los derechos y deberes tanto del tutor académico como del tutor de la entidad colaboradora.

Así pues, difícilmente se puede defender que en este caso la entidad colaboradora trate los datos personales de los alumnos únicamente siguiendo las instrucciones de las

universidades. Igualmente, es prácticamente imposible que la entidad colaboradora pueda proceder a suprimir o devolver los datos personales a la universidad "una vez finalice la prestación de los servicios de tratamiento". Pensemos nuevamente en el caso del hospital u otro tipo de centro sanitario en el que los datos de los alumnos acaben anotados en la historia clínica de un paciente. El hospital tiene que conservar esos datos durante el plazo legal en que ha de conservar la historia clínica y no puede proceder a suprimirlos porque hayan finalizado las prácticas.

Por tanto, en el caso de las prácticas universitarias, la universidad no contrata a otra entidad para que trate datos personales por su cuenta, sino que solicita la colaboración de otras entidades para que sus alumnos puedan realizar prácticas curriculares o extracurriculares, asumiendo ambas entidades las respectivas obligaciones que les impone la normativa reguladora de dichas prácticas.

La Agencia Española de Protección de Datos (AEPD) ya se ha pronunciado en varias ocasiones —a raíz de las consultas efectuadas por diversas universidades— sobre esta cuestión, resolviendo que las entidades colaboradoras en las que los alumnos realicen sus prácticas no pueden ser consideradas encargadas de tratamiento. Tampoco aprecia la AEPD que haya un caso de corresponsabilidad. Así pues, la Agencia considera que la entidad colaboradora es responsable del tratamiento, conforme a la definición que de dicha figura proporciona el artículo 4.7 RGPD: "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; […]".

Este criterio lo recoge la Agencia en el propio convenio que suscribió en 2019 con una universidad para la realización de prácticas por parte de los alumnos de títulos propios de máster y máster oficiales y que se publicó en el B.O.E. de 25 de octubre de 2019. Señala la cláusula duodécima de este convenio: "[…] La AEPD tiene la consideración de responsable del tratamiento de los datos personales de los alumnos comunicados por la Universidad […], ya que determina los medios y los fines de los tratamientos de datos necesarios para la realización de las prácticas universitarias que constituyen el objeto de este Convenio".

Se trata, pues, de una comunicación o cesión de datos y no de un contrato de encargo de tratamiento o de corresponsabilidad.

* Raquel Sánchez Rodríguez es abogada y Delegada de Protección de Datos de la Universidad Francisco de Vitoria.

21.06.2022. 70.000 € de multa por consultar si el abogado que iba a contratar arrastraba deudas. FUENTE: economistjurist.es

La Agencia Española de Protección de Datos ha multado con 70.000 euros a una empresa que, en el trascurso de un proceso de selección de un abogado, comprobó si uno de los candidatos aparecía en un fichero de morosos.

Alquiler Seguro, una empresa española dedicada a la gestión integral del alquiler de vivienda, ofertó a través de InfoJobs una vacante para un puesto de abogado.

Un interesado en ocupar el aludido puesto de trabajo se inscribió en dicha oferta.

Sin embargo, el citado aspirante tuvo conocimiento de que la empresa, antes de llamarle, hizo una consulta en un fichero de morosos (Asnef) para conocer de su situación financiera.

Consecuencia de lo anterior, el afectado interpuso una reclamación ante la AEPD argumentando que la compañía había consultado sus datos personales no para valorar la situación patrimonial a raíz de una futura relación comercial, de crédito o de pago periódico o aplazado (esta es la finalidad del tratamiento del fichero), sino que lo hizo en el marco de un proceso de selección de personal.

Así pues, como la mercantil reclamada en ningún momento recabó el consentimiento del aspirante ni tampoco le informó de que hicieron tal consulta, el reclamante razona que la empresa incurrió en una infracción por cuanto el tratamiento de los datos personales se había efectuado para una finalidad diferente de la prevista legalmente.

Argumentos de la empresa
Una vez que la AEPD dio traslado de dicha reclamación a la parte reclamada para que procediese a su análisis e informase a la primera de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos, la compañía respondió manifestando que el reclamante era un candidato que había sido descartado durante un proceso de selección de la mercantil y cuyos datos personales ya fueron destruidos.

Desde la empresa reclamada anunciaron que dentro de sus protocolos o procedimientos de selección de personal se establecen consultas a ficheros empresariales para puestos de gran responsabilidad o para cargos de personas colegiadas, siendo este tratamiento lícito y habitual en el caso de empresarios individuales y profesiones liberales, entre las que se encuentra la abogacía.

Además, la compañía expuso que este conflicto ha sido ocasionado debido a un posible error humano. Es decir, el técnico de selección debió de confundir el apartado de la plataforma Asnef, y en vez de introducir el DNI del candidato en “Asnef empresas” lo introdujo en “Servicio Bureau Crédito”.

La empresa reconoce su responsabilidad

Tras admitir a trámite la reclamación presentada por el candidato afectado, la AEPD adelantó que, sin perjuicio de lo que resultase en la fase de instrucción, los hechos aquí acontecidos podrían ser constitutivos de una infracción por vulneración del art. 6.1 del RGPD.

En palabras de la Agencia, “la documentación obrante en el expediente ofrece indicios evidentes de que la parte reclamada vulneró el art. 6 del RGPD, puesto que no consta base legitimadora para el tratamiento de los datos personales de la parte reclamante”.

El art. 20 de la LOPDGDD establece un catálogo de criterios de prevalencia del interés legítimo en el tratamiento de los datos de las personas físicas en los sistemas de información crediticia, sean profesionales liberales, empresarios individuales o no. Pues bien, en el supuesto aquí examinado, el tratamiento de datos personales no se presume lícito porque la compañía no ha indicado cuál es su interés legítimo, no ha aportado una ponderación que permita acreditar la prevalencia de tal interés y tampoco ha facilitado información al reclamante sobre la posibilidad de consulta.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, la institución dirigida por Mar España Martí ha tenido en cuenta como circunstancia agravante "la evidente vinculación entre la actividad empresarial de la reclamada y el tratamiento de datos personales de candidatos en los procesos de selección, clientes y terceros".

En este sentido, sin perjuicio de lo que se acordase en fase de instrucción, la Agencia fijó inicialmente la sanción a imponer en la cifra de 70.000 euros. No obstante, tras iniciar el procedimiento sancionador, a inicios del pasado mes de abril, Alquiler Seguro ha reconocido su responsabilidad y ha pagado voluntariamente la cuantía de 42.000 euros, haciendo uso de las dos reducciones previstas legalmente (reducción del 20% por reconocimiento de responsabilidad y reducción del 20% por pago voluntario).

27.06.2022. Sanción de la AEPD al BBVA por incumplimiento del RGPD. FUENTE: hosteltur.es

La Agencia Española de Protección de Datos sanciona con 48.000€ al BBVA por incumplir con el Reglamento General de Protección de Datos, concretamente los artículos art. 5.1.f), que expone que los datos personales serán tratados de tal manera que se garantice la confidencialidad e integridad, y el art. 32 relativo a la seguridad del tratamiento de los datos.

La AEPD concreta que el BBVA, como responsable del tratamiento, tendría que implementar medidas adecuadas para evitar la exposición de datos personales a terceros no autorizados y dado que en el presente caso se produce la brecha de confidencialidad, suponen que no se habían adoptado las medidas adecuadas.

Por otro lado, la entidad tendría que tener experiencia suficiente y contar con el adecuado conocimiento para el tratamiento de dichos datos, dado el elevado número de clientes con el que cuenta y el manejo de un importante registro de datos personales.

En definitiva, se sanciona a la entidad por producirse una brecha de confidencialidad y no disponer de medidas técnicas u organizativas que hubieran prevenido dicha situación.

En este caso, un usuario realizó en un cajero automático del BBVA un ingreso habitual en concepto de alquiler a la propietaria del piso que habitaba.

A diferencia de otras anteriores, el cajero no le facilitó ningún comprobante del ingreso, por ello, el hombre entró en la oficina del banco para que se lo facilitasen, cometiendo esta vez, uno de los empleados de caja del banco un nuevo error: en el documento que le

facilitaron constaba el saldo de la cuenta de la propietaria del inmueble, quién tras tener conocimiento de lo sucedido, interpuso una reclamación ante la AEPD.

Al disculparse y reconocer su error, pagando de forma voluntaria y adoptando las medidas adecuadas para que no se repita el error, el banco se acoge a dos de las reducciones previstas legalmente, la reducción del 20% por reconocimiento de responsabilidad y la reducción del 20% por pago voluntario, por lo que recibe un 40% de descuenta respecto de la sanción inicialmente impuesta de 80.000€.

29.06.2022. El Constitucional afianza el derecho al olvido en internet. FUENTE: elpais.com

El Constitucional ha dictado una sentencia que afianza el derecho al olvido en Internet. Por nueve votos a dos, el tribunal ha considerado que se han vulnerado derechos fundamentales de un comerciante, por los comentarios de descalificación de su actividad profesional vertidos en las páginas de servidores fuera de la Unión Europea, accesibles a través del buscador de motor en Internet Google. El fallo estima que el mantenimiento de esos enlaces no cumple los parámetros de interés público ni de tener una data suficientemente actual.

Con esta sentencia se anulan dos anteriores de la Audiencia Nacional y del Tribunal Supremo, respectivamente. Ambas resoluciones anularon a su vez la decisión inicial de la Agencia Española de Protección de Datos (AEPD), que había amparado al recurrente en su solicitud de supresión de ciertos datos que resultaban descalificatorios de su actividad profesional. Tales datos fueron publicados en portales de queja situados en los Estados Unidos, y a los que se accedía en España a través del buscador de motor en internet Google.

El Constitucional se refiere en primer lugar a su propia doctrina sobre el reconocimiento del derecho al olvido, sobre el que ya se pronunció en la sentencia 58/2018, en aquella ocasión en relación con la hemeroteca de un diario digital. En este caso, lo sustancial del nuevo fallo es que significa que el buscador Google no puede seguir vinculando el nombre del recurrente con la queja que presentó de forma anónima una ciudadana particular en una página web de Arizona, eliminando en consecuencia el enlace a esa página.

El tribunal ha concedido el amparo al recurrente en reconocimiento del derecho a la protección de datos del art. 18.4 de la Constitución, en relación con el derecho a la supresión de datos (derecho al olvido) del art. 17 del Reglamento General de Protección de Datos de la Unión Europea. A este respecto, el fallo precisa cuáles son los límites del derecho al olvido, entre los que destacan el factor de la importancia pública de la noticia y el de su antigüedad.

También pondera la responsabilidad de las entidades que operan motores de búsqueda de Internet y ponen a disposición de los internautas datos e informaciones vertidas en páginas de la red. La sentencia estima que tales entidades deben respetar el derecho a la supresión de esos enlaces, cuando infrinjan la normativa de la Unión Europea y española en la materia.

La resolución considera que se ha vulnerado el derecho fundamental que invoca el recurrente, puesto que los comentarios de descalificación de su actividad profesional vertidos en las páginas de servidores fuera de la Unión Europea no cumplían los parámetros de interés público ni de tener una data suficientemente actual que justificase el mantenimiento de los enlaces para acceder a ella. En consecuencia, se estima la demanda, declarando la indicada vulneración del derecho a la protección de los datos personales, con nulidad de las sentencias recurridas, sin que sea necesario adoptar otras medidas de reparación del derecho, no pedidas por el recurrente.

Los magistrados Juan Antonio Xiol y María Luisa Balaguer han anunciado un voto particular, por estimar que el recurso de amparo no debió prosperar, ya que a su juicio la información sobre las actividades comerciales del recurrente podía ser de interés para los consumidores. Por otra parte, en este asunto se ha ponderado también la posible colisión de derechos, entre el mencionado al olvido y el de la libertad de expresión de la particular que criticó la labor comercial del recurrente. Para la mayoría del tribunal debía primar en este caso el primero de estos derechos, al considerar que no quedaba afectado el derecho a la libertad de expresión, porque ya se expresó hace diez años al formular su queja. Por otra parte, tal descalificación seguirá figurando en la página web a la que se envió, de modo que simplemente no podrá asociarse directamente al nombre del recurrente y no figurará en su perfil digital.

JULIO

18.06.2022. Más de 20 millones en multas por privacidad en lo que va del año. FUENTE. Cincodias.elpais.com

Las cifras hablan por sí solas. La cuantía de las multas impuestas por la Agencia Española de Protección de Datos (AEPD) en estos primeros seis meses, casi 20,5 millones, está cerca de alcanzar dos tercios del total de las contabilizadas en todo 2021, 35 millones de euros. De acuerdo con la información recogida por La Ley en base a la información publicada por la AEPD, estas cifras parecen confirmar la escalada sancionadora en esta materia desde 2018, año en que entró en vigor el Reglamento General de Protección de Datos (RGPD). Es más, según la última memoria anual de la agencia, el salto de 2020 a 2021 supuso un incremento del 337%.

Unos datos que “impresionan”, afirma Paloma Bru, socia del departamento de TMT de Pinsent en Madrid. Tal y como valora la abogada, “al igual que ha ocurrido en otros países europeos, podemos confirmar una tendencia alcista de la actividad sancionadora de la autoridad de protección de datos”.

Mismo análisis comparte Paula Garralón, asociada del departamento de comercial y privacidad y protección de datos de Bird & Bird: “La AEPD es una de las autoridades europeas con una actividad sancionadora más elevada”. Esta intensa labor, añade Bru, “ha hecho que las empresas, de cualquier sector, coloquen en su mapa de ruta el cumplimiento de la protección de datos como uno de los riesgos que hay que abordar”.

Y es que las multas por privacidad se han convertido en un auténtico quebradero de cabeza para las empresas. El récord hasta la fecha lo ostenta Google, que fue sancionada

en mayo de este año con 10 millones de euros por obstaculizar el derecho al olvido de los usuarios. La agencia concluyó que el formulario que el gigante tecnológico utilizaba para las peticiones ciudadanas era confuso y supuso el traslado de sus datos a un banco que recopila violaciones de copyright. “El segundo semestre del año probablemente continúe con esta tendencia, multas ejemplificadoras especialmente a aquellas compañías que concentran altas cuota de negocio en su sector”, vaticina Garralón.

Por áreas.
Por otro lado, los ciudadanos también denuncian cada vez más las infracciones de protección de datos. El canal de denuncias de la agencia recibe año a año más comunicaciones, sobre todo en materia de videovigilancia, por instalar cámaras sin permiso o sin contar con las medidas de protección al usuario establecidas en la ley. Se trata del sector más multado del periodo, con 53 resoluciones de las cuales 33 acabaron con sanción. Sin embargo, el importe total de las multas en esta área suma poco más de 220.000 euros, con sanciones que van desde los 180 euros a un locutorio por colocar un sistema de videovigilancia sin cartel informativo, hasta los 170.000 euros a Mercadona por no proporcionar a la víctima de un accidente el vídeo de las cámaras de videovigilancia en el que aparecía el suceso. “Las empresas deben tener en cuenta que la instalación de sistemas de videovigilancia no supone carta blanca para poder grabar cualquier área y utilizar las imágenes captadas con fines diferentes a los de seguridad”, señala Bru. Por ello, agrega la experta, es necesario que, antes de instalar estos sistemas, las organizaciones realicen el correspondiente análisis de riesgos y determinen las medidas prácticas que deben cumplir.

Asimismo, por primera vez en 2022, la AEPD ha estimado los primeros recursos de reposición, anulando así cinco sanciones impuestas precisamente en el sector de la videovigilancia. En estos casos, sí se cumplía con la normativa, ya fuera porque las cámaras estaban bien señalizadas o porque simplemente no estaban funcionando y su instalación solo era disuasoria.

Los servicios de internet se sitúan en segundo lugar en cuanto a número de sanciones impuestas por la AEPD, con 24, aunque ostentan la primera posición en cuanto a cuantía total de las multas debido a los 10 millones de euros impuestos a Google. Las demás sanciones de este sector apenas suman 119.000 euros. Le sigue la contratación fraudulenta, área que cuenta con diez sanciones que suman 5,8 millones de euros. Muy de cerca, también con diez multas, aunque de mucha menor cuantía, algo más de 340.000 euros, se encuentra el sector de la publicidad a través de e-mail o móvil. En el quinto puesto están los asuntos laborales, cuyas siete multas ascienden a 2,2 millones de euros.

Por tipo de infracción
Del informe elaborado por La Ley también se desprende que en estos primeros seis meses de 2022 las obligaciones más vulneradas del RGPD son las relacionadas con la regla de la minimización, es decir, que las empresas se excedan pidiendo al usuario más datos de los necesarios para el fin concreto. El tratamiento ilícito de estos también es una de las infracciones más habituales de las organizaciones, bien por no contar con el consentimiento de la persona para usarlos para un propósito específico, o bien porque se exceden en el tratamiento de los mismos. Otra de las conductas más castigadas en estos

meses ha sido no facilitar la información suficiente al interesado sobre el tratamiento que se va a hacer de sus datos.

Esta realidad evidencia, según Garralón, que, pese a que el RGPD es plenamente aplicable desde hace cuatro años, las empresas siguen aprendiendo y adaptando sus procesos a la normativa. “Se trata de una carrera de fondo donde el objetivo es lograr el equilibrio entre el cumplimiento de la norma y el éxito del negocio”, concluye la abogada. Las compañías, según constatan desde el despacho de Bru, se han empezado a poner las pilas: “Hemos observado cómo, a diferencia de lo que ocurría años atrás, las empresas dedican recursos, tanto legales como organizativos y técnicos, para fomentar el cumplimiento normativo en privacidad”.

Amonestaciones
Pese a que la AEPD no puede multar a las Administraciones públicas, el organismo continúa apercibiéndolas por incumplimientos en materia de privacidad. Así, este año la agencia ha amonestado a distintas entidades por exponer datos personales sin consentimiento o por desoír las peticiones de los usuarios de suprimir esta información, entre otros motivos.

En enero, advirtió al Ayuntamiento de Ourense (Galicia) por haber colgado en el tablón de la Jefatura de la Policía Local los datos personales de algunos trabajadores al publicar los periodos vacacionales que se les habían denegado. Ese mismo mes, se amonestó al Ayuntamiento de Sotoserrano (Salamanca) porque uno de sus concejales difundió, al reenviar por WhatsApp, un escrito por el que se solicitaba la retirada de tierra depositada alrededor de la tumba del padre del reclamante. Según alegó el consistorio, se debió a un intento de evitar un conflicto familiar entre la parte reclamante y sus primos. En febrero, el apercibido fue el Ayuntamiento de Villafranca de los Barros (Badajoz), por tirar a los contenedores documentos con datos personales sin haber tenido en cuenta los protocolos para desechar papel establecidos para estas ocasiones.

Tampoco se libró el Consejo General del Poder Judicial (CGPJ). El órgano de gobierno de los jueces fue apercibido por exponer datos personales de los magistrados en su web, como información curricular o de bajas médicas, a través del Portal de Transparencia. La AEPD también tiró de las orejas al CGPJ por no haber verificado que los buscadores ya no recogían la URL.

TOP 10 DE SANCIONES EN EUROPA
746 millones. Según recoge el informe ‘Sanciones en RGPD’ elaborado por Ecix Group, Luxemburgo ocupa el primer puesto en el ranking de sanciones por privacidad en Europa. Multó a Amazon con 746 millones de euros en julio de 2021.
225 millones. Irlanda aparece en segunda posición. Sancionó con 225 millones de euros a WhatsApp en septiembre de 2021.
90 millones. El tercer puesto es para Francia, que sancionó con 90 millones de euros a Google por incumplir la normativa de cookies en diciembre de 2021.
60 millones. Francia también multó a Facebook en diciembre de 2021 por no permitir el rechazo de las cookies con 60 millones de euros.

60 millones. Según la agencia francesa, Google vulneró la privacidad de sus usuarios instalando cookies, por lo que recibió una multa de 60 millones de euros en diciembre de 2021.
50 millones. Francia sancionó con 50 millones de euros a Facebook en enero de 2021.
35 millones. Alemania multó en octubre de 2020 a H&M por recopilar información de la vida privada de algunos empleados.
27, 8 millones. Italia sancionó en enero de 2020 a TIM por no solicitar el consentimiento correctamente ni disponer de medidas de seguridad.
26,5 millones. Italia multó en diciembre de 2021 a Enel Energía por realizar llamadas promocionales de manera indiscriminada.
22 millones. Reino Unido sancionó en octubre de 2020 a British Airways debido a una brecha de seguridad en la que se expusieron datos de 500.000 clientes.

18.07.2022. Qué es la lista Robinson. FUENTE: publico.es

Si estás cansado de que te llamen por teléfono para ofrecerte ofertas de la más diversa índole o de recibir publicidad a través de tus cuentas de correo electrónico sin que hayas dado autorización ni permiso, seguro que te interesa todo lo que concierne a la Lista Robinson.

Y es que a través de ella puedes librarte de todos esos comerciales y avisos tan molestos que tan poco te interesan. Te explicamos qué es la Lista Robinson y qué tienes que hacer si deseas formar parte de ella.

La Lista Robinson
Conocido como la Lista Robinson, este es un servicio gratuito de exclusión publicitaria que está a disposición de todos los consumidores para que la publicidad que reciban desaparezca o disminuya considerablemente. Las empresas pueden acceder a él previo pago.

La Agencia Española de Protección de Datos determina que aquellas deben consultarlo, puesto que tienen la obligación de excluir de sus campañas publicitarias a todas las personas que estén incluidas en la Lista Robinson.

Como curiosidad, has de saber que el nombre de este listado procede de la novela de Robinson Crusoe, de Daniel Defoe. Esta denominación también suele usarse en los países anglosajones, como metáfora de alguien que quiere aislarse de la publicidad.

Cómo darse de alta en la Lista Robinson
Son muchas las personas que se han dado ya de alta en la Lista Robinson, en torno a 570.000, para evitar que los llamen por teléfono con fines publicitarios o comerciales o mediante el correo electrónico.

Si te interesa darte de alta en la Lista Robinson el trámite gratuito es muy sencillo, pues se trata de un simple formulario online de registro que deberás rellenar. Después te llegará un correo electrónico para activar tu perfil en la página. El responsable del tratamiento de datos que aportes es la Asociación Española de la Economía Digital (Adigital), gestora

del servicio, que cuenta con la autorización de la Agencia Española de Protección de Datos (AEPD).

Los datos que deberás aportar en el momento de darte de alta en la web son el nombre, el número de Documento Nacional de Identidad (DNI), un correo electrónico y la fecha de nacimiento. Luego podrás seleccionar cuáles son los medios mediante los cuales no quieres recibir publicidad para que las empresas dejen de molestarte. Así, deberás marcar todos o solo los que te interesen de entre el teléfono móvil, el teléfono fijo, el correo electrónico, SMS, MMS y el correo postal.

Efectividad de la Lista Robinson

Una vez te hayas inscrito, solo podrán mandarte ofertas y anuncios publicitarios aquellas empresas a las que hayas autorizado o de las que seas cliente. Recuerda que las empresas tienen la obligación de recabar esa autorización de forma expresa, clara e inequívoca, tal y como señala la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

La inscripción en la Lista Robinson es gratuita y voluntaria para las personas físicas. El trámite para los menores de 14 años deben realizarlo los padres o tutores legales. Una vez que te inscribas, surtirá efecto en un plazo de dos meses.

Ten en cuenta que las empresas con las que sí has tenido relación como cliente, a través de compras en tiendas online o físicas habiendo cedido tus datos, o hayas autorizado a través de cualquier medio, como suscripciones a newsletters o tarjetas de cliente, podrán seguir enviándote publicidad. Para librarte de estos anuncios, deberás dirigirte específicamente a la empresa para informarles de que ya no quieres recibir más publicidad ni notificaciones, amparándote en tus derechos.

Recomendaciones de la AEPD

En todo caso, con o sin inclusión en la Lista Robinson, la Agencia Española de Protección de Datos (AEPD) emite una serie de recomendaciones para evitar en la medida de los posible que nos molesten e inunden con publicidad. Así, has de recordar que, a la hora de efectuar una compra online o realizar una consulta o contratar un servicio, debes marcar la casilla que indica expresamente que no quieres recibir publicidad. Si no lo has hecho o no la encuentras, remite un correo electrónico o un SMS a la dirección que indiquen, que suele estar en la parte inferior de los envíos en tamaño muy pequeño y, a menudo, en cursiva.

Cuando navegues por internet y entres en determinada web o cuando te descargas aplicaciones en el móvil, verás con frecuencia que se te pide el consentimiento para enviarte publicidad. No marques esa casilla y no lo concedas. Para el caso de que desees hacerlo, ten en cuenta también que puedes revocar ese consentimiento cuando quieras.

Para hacerlo, si desconoces a quién tienes que dirigirte, y en la publicidad o documento que te envían no aparece, solo debes solicitar información a la persona que figura como responsable del tratamiento de datos con fines publicitarios o bien consultar en la página web el apartado sobre protección de datos, que es obligatorio que figure.

26.07.2022. Multa de 220.000 euros a DKV Seguros por enviar correos con datos de pruebas médicas a terceros. FUENTE: elconfidencialdigital.com

La Agencia Española de Protección de Datos (AEPD) ha multado a DKV Seguros con 220.000 euros por enviar a una mujer correos electrónicos con información privada de otras personas.

La empresa finalmente pagó 132.000 euros debido a que reconoció el error y realizó el pago de forma inmediata, lo que supuso una reducción del 40%.

Nombre, apellidos, número de póliza…
Según una resolución consultada por Confidencial Digital, una mujer puso en conocimiento de la AEPD que llevaba un año recibiendo en su dirección de correo electrónico autorizaciones de pruebas médicas de personas desconocidas.

En el contenido del mensaje aparecían datos como nombres, apellidos, número de póliza y, en ocasiones, el tipo de prueba diagnóstica al que tenían que someterse.

La mujer, cada vez que recibía este tipo de correos, dejaba constancia de que esa información no le correspondía a ella y que se la estaban enviando de forma equivocada, pero la aseguradora no solventó el problema.

51 correos y 32 afectados
DKV Seguros remitió desde el 16 de abril de 2020 al 9 de marzo de 2021, un total de 51 correos electrónicos en los que había informaciones de 32 personas.

Tras comprobar los hechos denunciados, la AEPD consideró que el tratamiento de los datos personales que realizó la parte reclamada no cumplía las condiciones que impone la normativa vigente en materia de protección de datos.

Configuración defectuosa del CRM
La AEPD destacó que el hecho de que trabajadores de dos encargados diferentes hayan cometido el mismo error, “demuestra que no se trata de un fallo humano concreto, sino de una defectuosa configuración del CRM (Gestión de Relaciones con el Cliente por sus siglas en inglés).

A ello añade que esto pone de manifiesto “que dichos errores son tan sólo la muestra de falta de medidas de seguridad adoptadas por el responsable”.

Asimismo, la resolución ha señalado que la aseguradora ha sufrido una brecha de seguridad de datos personales teniendo constancia de ella y no lo ha notificado a la Agencia.

Según el artículo 33 del Reglamento General de Protección de Datos, si una empresa tiene conocimiento de una brecha de seguridad, debe comunicarlo en 72 horas a la Agencia y, si no lo hace, debe adjuntar un justificante con los motivos de la dilación.

Pago voluntario y reconocimiento del error

Por todo ello, la AEPD ha sancionado a la aseguradora con 220.000 euros por la infracción de los artículos 5.1 (100.000 euros), 32 (60.000 euros) y 33 (60.000 euros) del RGPD. Tras reconocer el fallo y pagar voluntariamente, finalmente la multa se ha reducido a 132.000 euros.

Para calcular la multa, La AEPD ha tenido en cuenta varios agravantes debido al número de afectados, a que la mujer que recibió los correos dejó constancia del error en numerosas ocasiones, la durabilidad de la infracción y que los datos estaban relacionados con asuntos de salud.

Puesta en marcha de medidas correctoras
Fuentes de DKV Seguros han explicado a Confidencial Digital que, desde que tuvieron conocimiento de los hechos, pusieron en marcha medidas correctoras para que esto no volviera a repetirse.

Ejemplo de estas medidas han sido la realización de "extensas auditorías internas, eliminando datos incorrectos y modificando algunas reglas en su CRM, se han actualizado los procesos de gestión, se ha reforzado el cifrado de autorizaciones y se ha anonimizado el encabezado en los correos" han apuntado a ECD.

Asimismo, han añadido que lamentan y asumen los hechos, por lo que se pusieron en contacto tanto con la reclamante como con las personas afectadas para explicarles lo sucedido y pedirles disculpas.

DKV ha relatado que las incidencias fueron consecuencia de un fallo en cadena, originado por un error humano, en el que se vieron implicados empleados, proveedores y plataformas de gestión de datos.

26.07.2022. Denuncia anónima o confidencial. FUENTE. Elderecho.com

El canal de denuncias anónimo permite las denuncias sin ningún tipo de identificación. El confidencial debe garantizar la preservación de los datos identificativos del denunciante.

¿Qué es el canal de denuncias?
El canal de denuncias es un instrumento esencial para el Compliance de una empresa. Permite a los empleados denunciar irregularidades y actos delictivos de la empresa u organización en violación al código de conducta establecido.

¿Es obligatorio tener un canal de denuncias?
El 17-12-2021 expiró el plazo para la transposición de la Directiva 2019/1937 (whistleblowing o canal de denuncias interno), que obliga a las empresas del sector jurídico con 50 o más trabajadores a la obligación de establecer canales de denuncia interna, con independencia de la naturaleza de su actividad, aunque la misma prevé una ampliación del plazo hasta el 17-12- 2023 para aquellas entidades del sector privado cuya plantilla comprenda entre 50 y 249 trabajadores.

Aquellas entidades jurídicas privadas cuya plantilla no supere los 50 trabajadores, pueden ser eximidas de la obligación de implantar canales y procedimientos de denuncia interna.

¿Es obligatorio que aparezcan mis datos en la denuncia?
En España, hasta la entrada en vigor de la nueva Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LO 3/2018), existía la controversia de si las denuncias realizadas por medio de canales internos debían permitir una denuncia de forma anónima, o si era necesario realizar la denuncia de manera nominativa, solicitando la identificación del denunciante.

Con la publicación de la Ley, queda clara la oferta de la opción de denuncia anónima, fundamental para poder recibir denuncias graves que de otra manera los trabajadores y colaboradores no se atreverían a señalar por temor a represalias en caso de ser identificados.

Protocolo del canal de denuncias internas
Cada empresa debe fijar un protocolo personalizado que tenga como finalidad establecer un sistema eficaz de gestión, investigación y respuesta de las posibles denuncias que puedan presentarse a través del canal de denuncias interno de o cualquier otro medio. De esta manera, se instaurará en la sociedad un proceso reglado de obligado seguimiento que comprenderá la actuación a llevar a cabo desde el momento en que una denuncia es interpuesta hasta que, en su caso, la persona denunciada sea sancionada, incluyendo, asimismo, la evaluación posterior de la incidencia y la proposición de medidas a implantar en la sociedad en el supuesto en el que sea considerado necesario.

¿Qué normativa se aplica a la implementación de un canal de denuncias?
El hecho de que el canal de denuncias sea una parte del cumplimiento del sistema de Compliance (CP art.31 bis) no exime de que este tenga que cumplir con la normativa en materia de protección de datos, al igual que ocurre con todo tratamiento de datos de carácter personal realizado en nuestro país y dentro de la UE.

La implementación del canal de denuncias en materia de protección de datos se rige por la siguiente normativa aplicable:

Directiva wistherblowing (Dir 2019/1937 art.6)
Aunque existe la obligación de garantizar el anonimato en el canal de denuncias, los Estados miembros mantienen la facultad para exigir o no a las personas jurídicas, tanto públicas como privadas, o a las autoridades competentes, aceptar la tramitación de dichas denuncias anónimas.

Una de las principales obligaciones que establece la directiva europea sobre protección de denunciantes es la creación de canales de denuncia internos. Estos pueden ser mediante sistemas en línea, vía telefónica, por correo postal o por cualquier otro medio de comunicación equivalente. Asimismo, se ha de garantizar la confidencialidad respecto a la identidad del denunciante, independientemente del canal de denuncias que haya empleado.

Sistemas de información de denuncias internas (LOPDGD art.24)

Es lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso a través de denuncia anónima, la realización de actos o conductas que puedan resultar contrarios a la normativa general o sectorial de aplicación. Los empleados y terceros deben ser informados acerca de la existencia de estos sistemas de información.

Acceso a los datos

Queda limitado exclusivamente a quienes desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen. No obstante, es lícito su acceso por otras personas que realicen funciones de gestión y control de recursos humanos, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales, sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo.

Garantía de confidencialidad

Deben adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que haya puesto los hechos en conocimiento de la entidad, en caso de que se haya identificado.

Conservación de datos en el sistema de denuncias

Los datos deben conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados. En todo caso, transcurridos tres meses desde la introducción de los datos, debe procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica.

Grupo de Trabajo del art.29 -actual CEPD- (Dictamen 1/2006)

Este órgano se postula hacia canales de denuncia abiertos, es decir, de manera identificada, fundamentándolo hasta en seis razones diferentes, pero a pesar de su preferencia, no rechaza de forma categórica la posibilidad de que se puedan dar denuncias de forma anónima.

Agencia Española de Protección de Datos (Informe 128/2007)

En el indicado informe se aconsejaba evitar la existencia de denuncias anónimas, garantizándose así la exactitud e integridad de la información contenida en dichos sistemas. Actualmente, este informe ha quedado superado por LOPD art.24, que sí permite la denuncia anónima.

Fiscalía General del Estado (Circular 1/2016)

Se indica la prohibición expresa de cualquier tipo de represalia contra los "whistleblowers" por parte de la entidad, lo cual crea una mayor seguridad jurídica en este ámbito. Asimismo, se debe garantizar que los denunciantes tengan acceso a información y asesoramiento completo, independiente y gratuita sobre los procedimientos y recursos disponibles, así como a asistencia jurídica durante los procedimientos.

29.07.2022. Google Chrome retrasa el final de uso de las cookies de terceros hasta 2024. FUENTE: directivosygerentes.es

El plan anterior pasaba por despedirse definitivamente de las cookies de terceros en 2023.

Google lleva meses trabajando para terminar con las cookies de terceros en su navegador Chrome. Para ello ha creado la iniciativa Privacy Sandbox, con la que busca desarrollar alternativas para la preservación de la privacidad online de los internautas.

Aunque hace un año la compañía explicaba que realizaría pruebas hasta finales de 2022 para despedirse definitivamente de las cookies entre mediados y finales de 2023, su plan vuelve a sufrir revisiones.

De esta forma, Google espera ahora que la disponibilidad general de las APIs de Privacy Sandbox se produzca en el tercer trimestre de 2023 y que las cookies comiencen a desaparecer de Chrome durante la segunda mitad de 2024, de manera gradual.

Del trabajo con desarrolladores, reguladores y otras partes implicadas, ha llegado a la conclusión de que hace falta más tiempo para evaluar las tecnologías de Privacy Sandbox. De ahí que se amplíe el periodo de pruebas, con el consecuente retraso en el adiós definitivo a las cookies.

Cabe destacar que los desarrolladores ya tienen acceso a las APIs y, a partir del próximo mes de agosto y hasta 2023, las pruebas se expandirán a otros usuarios.

Más del 45% de internet sin cookies
"El anuncio de Google puede ser un indicio de que la compañía considera que no hay suficientes empresas que hayan iniciado la transición hacia un modelo alternativo sin cookies", comenta sobre esta decisión Travis Clinger, vicepresidente sénior de Addressability & Activations de la plataforma de conectividad de datos LiveRamp.

"Independientemente del plazo que haya establecido Google, más del 45% de internet ya no tiene cookies, las aplicaciones móviles no tienen cookies y la CTV (TV conectada) no tiene cookies", enumera.

En su opinión, "ha llegado el momento de que los editores y marketers controlen su destino y den el paso desde la identidad basada en cookies a la identidad basada en personas".

"Hacer el cambio a su opción preferida sin cookies ahora le permite beneficiarse de la escala de las cookies de terceros mientras todavía existen, y también llegar a los consumidores en entornos ya sin cookies", indica. "Esto puede ser tan fácil como pulsar

un interruptor en su DSP o SSP, o desplegar un código sencillo. Retrasar el movimiento sólo significa seguir engañándose a sí mismo para obtener un mejor rendimiento".

"Dada la incertidumbre económica actual, es especialmente importante optimizar el impacto de cada dólar de marketing y publicidad", ahonda Clinger.

"Los profesionales del marketing deberían preguntarse si sus inversiones son abordables, responsables y medibles. Aquellos que están avanzando en su futuro sin cookies y negociando en base a los resultados del negocio, en lugar de las métricas tradicionales de alcance y conciencia", observa, "pueden asegurar que sus inversiones en media están funcionando más que nunca".

AGOSTO

30.08.2022. La San Silvestre, multada por pedir el pasaporte Covid o una prueba PCR a sus participantes FUENTE: 20minutos.es

La empresa Last Lap, organizadora de la San Silvestre Vallecana, ha abonado 9.600 euros de multa por solicitar el pasaporte Covid, o prueba PCR complementaria antes de la carrera, a todos los participantes que se inscribieron en la tradicional prueba de fin de año, que se celebró el 31 de diciembre de 2021.

La multa ha sido impuesta por la Agencia Española de Protección de Datos (AEPD), que ha dado la razón a 'Liberum', una asociación ciudadana creada expresamente para "restaurar los derechos y libertades" desde la pandemia por la Covid-19 y tras la denuncia que presentaron el pasado 31 de enero, un mes después de la carrera.

La denuncia prosperó, según ha podido saber Europa Press, después de que Last Lap haya infringido los artículos 6 y 9.2 del Reglamento General de Protección de Datos (RGPD), éste último define las excepciones de prohibición de tratamiento de datos. Este caso, el de una carrera de atletismo, no aparece como excepción.

De esta forma, la San Silvestre no debió solicitar esta información al no tener competencias, aunque sus bases de competición incluyesen dicha cláusula. "En ningún momento, puede ser el consentimiento la base que legitime este tratamiento de datos, ya que, en este caso, cualquier usuario registrado podría negarse a facilitar estas evidencias, participar en la carrera estando contagiado por la Covid-19 y contagiar a otros participantes", añade la AEPD.

Así, la AEPD confirmó que la parte reclamada procedió al pago de la sanción "en la cuantía de 9.600 euros haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

"El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio", sentencia la resolución.

18.08.2022. La gobernanza de datos europea. FUENTE: empresaactual.es

Tal como indica la Comisión Europea, la Estrategia Europea de Datos busca convertir a la Unión en líder de una sociedad dirigida por los datos. La creación de un mercado único de datos permitirá que estos fluyan libremente por la Unión y entre sectores, en beneficio de las empresas, los investigadores y las administraciones públicas. Hablamos de la gobernanza de datos.

Los datos son el eje principal de la transformación digital. El acceso al ingente volumen de datos y su procesamiento son esenciales para la innovación y el crecimiento. De hecho, dicha innovación basada en los datos ofrece beneficios tanto a la ciudadanía como a la economía europeas.

La gobernanza de datos
El pasado mayo, el Consejo de la Unión Europea aprobó la Data Governance Act (DGA), resultado de la propuesta de la Comisión Europea de finales de 2020.

El Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos establece unos mecanismos sólidos que facilitarán la reutilización de determinadas categorías de datos protegidos del sector público, aumentarán la confianza en los servicios de intermediación de datos y fomentarán la cesión altruista de datos en toda la UE.

Se trata de un componente importante de la Estrategia Europea de Datos, cuyo objetivo es reforzar la economía de los datos.

Ámbitos de la gobernanza de datos
La nueva normativa regula cinco grandes ámbitos:

La cesión de determinadas categorías de datos protegidos en posesión de organismos del sector público para su reutilización
La DGA tiene por objeto ser un mecanismo que permita la reutilización de determinadas tipologías de datos de los organismos del sector público, sujetos a derechos de terceros (por ejemplo, secretos empresariales, información confidencial interna, estadísticas confidenciales, datos protegidos por derechos de propiedad intelectual o datos personales), con ciertas condiciones especiales que deben cumplirse:

Las autoridades públicas con competencias para permitir o denegar la reutilización de los datos, deben hacer públicas las condiciones para dicha reutilización, bajo criterios de transparencia, no discriminación, proporción y objetividad.
Estas autoridades están obligadas a preservar la naturaleza de los datos que van a ser reutilizados. Para ello, se establecen algunos requisitos:

1. Anonimización de datos personales y tratamiento necesario de datos que contengan información comercial confidencial.
2. Generar un entorno de tratamiento seguro y controlado por dicho organismo público, para su acceso tanto a distancia como físicamente.

Los acuerdos exclusivos para la reutilización de los datos del sector público deberán estar justificados y ser necesarios para la prestación de un servicio o un producto con interés general, y sin que exista cualquier otra alternativa. En cuanto a los plazos, habrá un límite de 30 meses para contratos ya existentes y de 12 meses para contratos nuevos.
La Comisión creará un punto de acceso único, con registro electrónico, de los datos del sector público.

Creación de proveedores de servicios de intermediación de datos
La DGA fomenta los servicios de intermediación de datos. Con ello, se busca establecer un entorno seguro en que empresas y particulares puedan compartir datos, garantizando su seguridad, disponibilidad, integridad y usabilidad.

La normativa establece condiciones para la provisión de dichos servicios de intermediación de datos:

Notificación previa para su registro.
No utilización de los datos por los servicios de intermediación para fines distintos de su puesta a disposición de los usuarios de datos.
Presentar un estatus neutral, debiendo distinguir la actividad de intercambio de datos de cualquier otra operación comercial que realicen, no pudiendo utilizar los datos para fines personales o comerciales.

Altruismo de datos
La DGA también facilita la puesta de datos a disposición del bien común, de forma voluntaria y altruista, con base en un formulario europeo, para permitir el uso de sus datos, sin solicitar contraprestación a cambio. Estos datos serían relevantes en temas relacionados con la lucha contra el cambio climático, la asistencia sanitaria, la producción y difusión de estadísticas oficiales, la investigación científica, etc.

European Data Innovation Board
La ley prevé la creación de un grupo de expertos: el Consejo Europeo de Innovación de Datos. Su objetivo principal es asesorar y asistir a la Comisión Europea en:

La mejora de la interoperabilidad de los servicios de intermediación de datos.
Garantizar la práctica coherente de altruismo de datos para toda la UE.
El desarrollo de directrices coherentes para el establecimiento de requisitos de ciberseguridad en el intercambio y almacenamiento de datos.

Acceso y transferencia internacional de datos no personales
La DGA establece medidas de salvaguardia para luchar contra las transferencias internacionales de datos ilícitas para los datos del sector público, los servicios de intermediación de datos y las organizaciones de altruismo de datos.

Estas medidas siguen la regulación ofrecida para los datos personales en el Reglamento General de Protección de Datos (RGPD), mediante la potencial adopción de decisiones de adecuación para aquellos países de fuera de la UE que ofrecen garantías adecuadas para el uso de los datos, o, en su ausencia, el establecimiento de cláusulas contractuales tipo.

La DGA será aplicable 15 meses después de su entrada en vigor, que tendrá lugar veinte días después de su publicación en el Diario Oficial de la UE.

24.08.2022. Existen apps infantiles que recopilan datos de menores ilegalmente. FUENTE: 20minutos.es

Los menores tienen acceso miles de aplicaciones infantiles con las que pueden entretenerse y aprender, sin embargo, que esas plataformas hayan sido desarrolladas para el público infantil no significa que sean seguras en lo que respecta a su privacidad.

El estudio 'Won't Somebody Think of the Children? Examining COPPA Compliance at Scale' señala que el 57% de las apps infantiles gratuitas más populares de Estados Unidos vulnera la privacidad de los menores. Además, el 19% almacenan identificaciones personales, a través de terceros sin ajustarse a los mecanismos de protección exigidos por la normativa.

Los desarrolladores de aplicaciones recopilan los datos, y con frecuencia utilizan un kit llamado 'SDK' para acceder a la información. Los usuarios deben estar informados sobre el tratamiento, además, contarán con una base legal para otorgar el consentimiento.

César Córcoles (profesor de los Estudios de Informática, Multimedia y Telecomunicación de la Universitat Oberta de Catalunya) afirma en el blog de Universitat Oberta de Catalunya (UOC) que "el problema es que muchas veces los desarrolladores no leen la licencia de ese SDK que están utilizando. Pero, si la leyeran, se darían cuenta de que están recopilando datos de niños, algo que podría ser ilegal".

UOC señala que "la información que recogen con mayor frecuencia es el identificador único, que es xxx@gmail.com o el correo que tenga, o bien el nombre de usuario. Con menos frecuencia, salvo en las aplicaciones de mensajería, tienen acceso a los contactos. Y, aunque también es posible que graben lo que se dice por el micrófono, por defecto la mayor parte de aplicaciones no tiene permiso para hacerlo".

¿Es legal?
El Reglamento General de Protección de Datos (RGPD) prevé que el consentimiento será válido a partir de los dieciséis años, por tanto, para tratar datos personales de menores de dieciséis años se deberá contar con la autorización de los padres o tutores legales.

En España, la nueva Ley Orgánica de Protección de Datos y garantía de derechos digitales (LOPDGDD) fijó los catorce años como edad mínima para consentir.

Córcoles añade que "en el 99% de las veces que se vulnera la privacidad del menor no hay mala intención, ya que los desarrolladores suelen recopilar esos datos para tener información de diagnóstico del funcionamiento de la aplicación. Y, afortunadamente, el desconocimiento o la falta de mala intención no exime de cumplir la ley".

Medidas para evitar la recopilación de datos

Los adultos pueden activar los controles parentales, quitar los permisos de acceso que no sean necesarios y elegir el mejor sistema operativo dependiendo del uso que le dé el menor al móvil.

27.08.2022. Multan a un partido político de Jaén por enviar correos masivos sin copia oculta. FUENTE: elconfidencial.com

La Agencia Española de Protección de Datos (AEPD) ha acordado sancionar al partido político Jaén Sentido y Común (JSC) con 2.000 euros de multa por enviar un correo electrónico a 241 personas con sus direcciones visibles y sin haber solicitado autorización previa a alguno de los destinatarios. Fue uno de ellos el que alertó de esta circunstancia después de que se pusiese en contacto con la formación política para que le informasen sobre el tratamiento de los datos personales y no recibir contestación al respecto.

En la resolución de la AEPD, a la que ha tenido acceso este periódico, se explica que el reclamante colaboró con el grupo municipal durante "el proceso de candidaturas para la alcaldía en la que concurrían varias organizaciones políticas", por lo que se intuye que fue fruto de esta relación previa por lo que JSC disponía de email y "sospecha que se podría haber producido un tratamiento o cesión de datos sin su autorización".

Esta persona expuso que el 26 de septiembre de 2021 recibió un correo electrónico remitido a 241 destinatarios "con las direcciones de todos ellos visibles", sin haber hecho uso de la función "con copia oculta (CCO)". En el mismo se convocaba a una "asamblea abierta" de Jaén Sentido y Común que debía celebrarse cuatro días más tarde.

El 28 de septiembre se dirigió a la formación política solicitando que acreditase la autorización para la utilización de su email para recibir estas comunicaciones y posteriormente pidió la vía de contacto con el Delegado de Protección de Datos (DPD). El requirente, según precisó en su escrito de reclamación, recibió "una contestación evasiva" y el partido le informó de que procedía a la eliminación de su dirección de correo electrónico de su lista de contactos. Este paso no le contentó e incidió en que no había recibido respuesta a su petición de información sobre el tratamiento realizado con su correo electrónico.

Por esta circunstancia decidió presentar una reclamación ante la Agencia Española de Protección de Datos y aportó como prueba una "copia del correo electrónico remitido donde figuran 241 destinatarios con las direcciones de todos ellos visibles". Se admitió a trámite y el pasado 18 de marzo se acordó iniciar proceso sancionador a Jaén Sentido y Común.

"La documentación obrante en el expediente ofrece indicios evidentes de que la parte reclamada vulneró el artículo 5 del Reglamento General de Protección de Datos (RGPD) —relativo al tratamiento, protección y seguridad de la información personal— al revelar a terceros datos de carácter personal", ya que se considera probado que se remitió una convocatoria de asamblea sin copia oculta. "Ello, por carecer de las medidas adecuadas de seguridad", como puede ser "el cifrado de datos personales".

El análisis del caso, según la AEPD, revela que "no consta acreditado" que la formación política adoptara las disposiciones técnicas y organizativas adecuadas conforme a lo exigido en la normativa, pues "se revela información y datos de carácter personal a terceros, con la consiguiente falta de diligencia por el responsable".

Con base en estas conclusiones, se acuerda imponerle dos sanciones. Una grave de 500 euros por supuestamente no garantizar un nivel de seguridad adecuado al riesgo; y otra de 1.500, considerada muy grave, por no adoptar iniciativas que aseguren la protección contra el tratamiento no autorizado o ilícito de los datos personales y contra su pérdida.

Además de estos 2.000 euros de multa en total, el organismo fiscalizador instaba a JSP a configurar el envío de correos de forma que se puedan remitir con copia oculta cuando se dirija a una pluralidad de interesados. Esto debía ser acreditado en un plazo de diez días hábiles para confirmarse el cese de la conducta infractora.

"Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva", concluye la resolución, contra la que se puede interponer recurso de reposición ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

SEPTIEMBRE

01.09.2022. 5.000 € de multa por no informar a una clienta sobre la gestión de sus datos. FUENTE: economistjurist.es

La Agencia Española de Protección de Datos ha sancionado con 5.000 euros a una inmobiliaria por no informar “convenientemente” a sus clientes de los fines a los que se destinarían los datos personales obtenidos de ellos.

El caso
En septiembre de 2021, una clienta de la inmobiliaria interpuso una reclamación en la AEPD en la que informaba que, tras realizar una reserva para la compra de un inmueble, la primera no rellenó ninguna cláusula ni fue informada del tratamiento de sus datos personales.

En particular, para justificar lo anterior, la parte reclamante aportó un documento de oferta de inmueble en el que aparecían los datos personales de la afectada, así como, los datos de la inmobiliaria. Sin embargo, como adelantábamos, no existía ninguna referencia o información sobre la gestión de los datos personales obtenidos por la mercantil.

Tras tener conocimiento de tal circunstancia, la Agencia trasladó la reclamación a la compañía reclamada para que diese respuesta a la misma.

Sin embargo, meses después, al no recibir contestación alguna a las solicitudes hechas desde la institución dirigida por Mar España Martí, la AEPD admitió a trámite la reclamación y ordenó incoar el correspondiente procedimiento sancionador a la parte reclamada, por la presunta infracción del art. 13 del RGPD, al existir indicios de la falta

de información ofrecida a los clientes sobre el tratamiento de sus datos personales, cuando éstos son obtenidos directamente de ellos.

5.000 euros de multa
En primer lugar, la Agencia recuerda que el considerando 61 del RGDP establece que se deberá facilitar a los interesados la información sobre el tratamiento de sus datos personales "en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso".

Tras detallar toda la información que se debe facilitar al interesado cuando los datos son recogidos directamente de él conforme a lo previsto en el art. 13 del mismo cuerpo legal, la Agencia alerta que, en el caso que aquí nos ocupa, la palpable ausencia de información por parte de la inmobiliaria sobre el tratamiento de los datos personales cuando se obtienen los datos personales de sus clientes supone la vulneración del citado precepto.

En este sentido, el art. 72.1.h) de la LOPDGDD, considera muy grave, a efectos de prescripción, "la omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los arts. 13 y 14 del RGPD".

Pues bien, de acuerdo con los preceptos indicados, a efectos de fijar el importe de la sanción a imponer, la AEPD considera que procede graduar la sanción conforme a la siguiente circunstancia agravante: la vinculación de la actividad del infractor con la realización de tratamientos de datos personales. En opinión de la Agencia, la reclamada administra, día a día, "datos personales de miles de interesados", al tener como actividad principal, la compraventa de muebles e inmuebles, promoción de edificaciones, obras y reformas, intermediador financiero, asesoría, administración, servicios a empresas, tasación y peritación, todos estos servicios relativos a la propiedad inmobiliaria. "Esta circunstancia determina un mayor grado de exigencia y profesionalidad y, consiguientemente, de responsabilidad de la entidad en relación con el tratamiento de los datos personales", advierte el organismo público creado en 1992.

Así las cosas, además de obligar a la inmobiliaria a implementar un mecanismo en la gestión de los servicios realizados donde se informe a los clientes del tratamiento que se realizará de sus datos personales, la AEPD termina imponiendo a la mercantil reclamada una multa de 5.000 euros, por la infracción del art. 13 del RGPD, "al no informar convenientemente a los clientes, de los fines a los que destinan los datos personales obtenidos de ellos".

06.09.2022. Multa de más de 400 millones a Instagram por la deficiente gestión de los datos de sus usuarios. FUENTE; lavanguardia.com

La tecnológica Meta ha recibido un nuevo batacazo: la Comisión Irlandesa de Protección de datos ha impuesto una multa de 405 millones de euros a Instagram. La sanción se debe a una violación del Reglamento General de Protección de datos (RGPD), siendo la segunda más alto de a historia por el mismo delito. En cuando a Meta, es la multa más alta jamás recibida por la tecnológica de Mark Zuckerberg.

En septiembre del año pasado la plataforma Facebook tuvo que hacer frente a una sanción que ascendía a los 225 millones de euros. Ahora, un año después, se enfrenta a una nueva multa por volver a incumplir el Reglamento General de Protección de datos. Instagram ha permitido a menores de edad tener acceso a cuentas comerciales, filtrándose sus direcciones de correo y números de teléfono.

Amazon recibió una multa en materia de RGPD - por recopilación de datos indebida - en julio de 2021 que ascendía a 746 millones de euros. En cuanto a la sanción impuesta a Instagram, no han trascendido los detalles, aunque se sabe que está relacionada con la violación de la privacidad de usuarios menores de edad. Al acceder a cuentas comerciales, los números de teléfono y direcciones de correo de estos usuarios han sido filtrados.

"Cualquier persona menor de 18 años tiene automáticamente su cuenta configurada en privada cuando se une a Instagram, por lo que solo las personas que conocen pueden ver lo que publican", declaraba Meta para la Comisión. La tecnológica aseguraba que, siempre y cuando especifiquen su edad real, los usuarios menores tenían por defecto configurada su cuenta como privada.

Meta, empresa matriz de Instagram, está a tiempo de realizar una apelación a la sanción de 405 millones de euros impuesta por la Comisión Irlandesa de Protección de datos. Esta no es la primera polémica que tiene Instagram respecto al tratamiento de datos de los usuarios menores de edad, cuya privacidad debería estar completamente asegurada.

La plataforma se vio obligada a cancelar el desarrollo de la herramienta 'Instagram Kids' tras el rechazo que generó entre los internautas. Puso en marcha múltiples funciones prometiendo que estas protegerían a los menores de edad y, recientemente, canceló la cuenta de la página porno Pornhub en Instagram, al estar investigándose casos de pornografía infantil en la misma.

07.09.2022. Sistema de videovigilancia y grabación de voz. FUENTE: elderecho.com

La AEPD analiza y responde a una consulta relacionada con la instalación de un sistema de videovigilancia en un ayuntamiento con fines de “Seguridad y control de acceso a edificios “y “control de presencia de empleados”, que genera diferentes dudas respecto a la captación de la imagen y la voz de las personas que acceden al edificio y de los trabajadores.

Desde el Ayuntamiento que plantea la consulta se cuestiona si deben ser atendidas las alegaciones de los trabajadores, que consideran la grabación de voz una vulneración del artículo 18.3 y 4 de la Constitución.

La imagen de la persona es un dato personal, y su tratamiento derivado de la captación y, en su caso, grabación, ha de ajustarse al Reglamento 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 y por el que se deroga la Directiva 95/46 (Reglamento General de Protección de Datos, en adelante “RGPD”), tal como indica la Agencia.

El RGDP define “datos personales” con una gran amplitud. Es por ello, que la imagen así como la voz de una persona se considera un dato personal, al igual que lo es cualquier información que permita determinar, directa o indirectamente, su identidad, como por ejemplo, una matrícula de vehículo, una dirección IP, etc. y así lo ha considerado en reiteradas ocasiones la AEPD.

Los sistemas de videovigilancia suponen un tratamiento de datos de carácter personal, y su instalación deberá respetar el principio de proporcionalidad, valorando así la posibilidad de adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

Así, El RGPD recoge en el artículo 5 como uno de los principios relativos al tratamiento, el principio de minimización de datos, de forma que los datos objeto de tratamiento sean adecuados, pertinentes y limitados en relación con los fines para los que son tratados.

La AEPD manifiesta que la instalación de cámaras de videovigilancia sería una medida proporcional y justificada si se cumplen estos requisitos:

1. Que se trate de una medida susceptible de conseguir el objetivo propuesto.
2. Que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia.
3. Que la misma sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto”.

En el supuesto planteado, el principio de proporcionalidad ha de considerar la captación y la grabación de la voz de las personas físicas junto con la grabación de la imagen a través de sistemas de videovigilancia.

A este respecto, la grabación del sonido de voz en un soporte informatizado constituye un almacenamiento de datos personales (tratamiento). Es decir, el hecho de que pueda resultar legítima la videovigilancia por razones de seguridad, no implica necesariamente que se legitime la grabación de la voz, tratamiento que tendría que tener su justificación propia.

En este sentido, y relacionándolo en el ámbito laboral, la Agencia Española de Protección de Datos menciona la sentencia del Tribunal Constitucional 98/2000 que censura la instalación de micrófonos en las zonas de caja y de ruleta francesa que quería realizar una empresa con el objetivo de grabar las conversaciones en esas zonas aludiendo a poder reforzar así la seguridad del casino y resolver las eventuales reclamaciones de los clientes. A juicio del Tribunal “la implantación del sistema de audición y grabación no ha sido en este caso conforme con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial, pues la finalidad que se persigue (dar un plus de seguridad, especialmente ante eventuales reclamaciones de los clientes) resulta desproporcionada para el sacrificio que implica del derecho a la intimidad de los trabajadores (e incluso de los clientes del casino). Este sistema permite captar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios ajenos

por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por la empresa. Se trata, en suma, de una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE, pues no existe argumento definitivo que autorice a la empresa a escuchar y grabar las conversaciones privadas que los trabajadores del casino mantengan entre sí o con los clientes".

Atendiendo a la doctrina descrita, la utilización del sistema de videovigilancia para grabar las conversaciones tanto de empleados, como de público en general que acuden a los edificios del Ayuntamiento en cuestión, en la medida que el sistema va a permitir captar comentarios privados, alega la AEPD que puede resultar incompatible con el principio de proporcionalidad referido anteriormente, y que debe ser cumplido.

En ese principio de proporcionalidad se encuentra recogido el derecho a la intimidad, honor y propia imagen de las personas, de forma que resultará desproporcionada la captación de imágenes que puedan afectar a dichos derechos o la escucha o grabación de conversaciones. La Agencia menciona, además, que la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, dispone en su artículo 7 que "Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:

Uno. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.

Dos. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción."

En consecuencia, la AEPD responde a la consulta que las grabaciones indiscriminadas de voz y conversaciones de los empleados y público en general que acceden a los edificios del Ayuntamiento a través de sistemas de videovigilancia, no cumpliría el principio de proporcionalidad, considerándose una medida intrusiva para la intimidad de los menores y para su derecho a la protección de datos de carácter personal.

14.09.2022. Multa de 10.000 euros a una firma de trajes por publicar una foto de una clienta. FUENTE: eldiariocantabria.publico.es

La Agencia Española de Protección de Datos (AEPD) ha multado con 10.000 euros a la firma de trajes de boda Sophie et Voilà por subir a su perfil de Instagram la foto de una de sus clientas, en la que aparecía con uno de sus vestidos, según ha recogido Facua.

La afectada interpuso en 2021 una reclamación ante la Agencia contra la empresa tras descubrir que había subida una foto suya. En ella, podían verse a dos personas, un hombre

y una mujer, posando y con la cara tapada por un círculo negro para evitar su identificación, aunque la reclamante se reconoció debido al vestido de boda.

Según consta en la resolución de la AEPD, Sophie et Voilà alegó en su respuesta a la reclamación que en ningún momento podía entenderse que las personas de la foto eran indentificables y que no existía, por tanto, un tratamiento de los datos personales de la afectada y su pareja. La firma señalana que la fotografía había sido deliberadamente alterada para ocultar la identidad, por lo que no podía considerarse un tratamiento ilícito de datos.

La Agencia, sin embargo, ha entendido que la empresa cometió una infracción del artículo 6 del Reglamento General de Protección de Datos Personales (RGPD) ya que las imágenes publicadas "eran identificables" y el objetivo de subirlas era "lograr que se procediese a su abono". Esto es porque Sophie et Voilà señaló que la fotografía sólo estuvo publicada una hora, hasta que la afectada le pagó el vestido.

El citado artículo del RGPD señala que el tratamiento de datos personales sólo será lícito si "el interesado dio su consentimiento [...] para uno o varios fines específicos", entre otros, circunstancia que la AEPD señala que no se produjo en este caso.

IMÁGENES

En contra de los argumentos de Sophie et Voilà, la Agencia ha determinado que las imágenes publicadas por la empresa sí eran identificables y que por eso "fueron publicadas en Instagram por la reclamada con la finalizad de cobrar por las ventas efectuadas". "En este sentido", continúa, "ha de indicarse que la falta de pago no legitima a la parte reclamada a utilizar las imágenes de las reclamantes, si no cuenta con su consentimiento expreso, por lo tanto se ha incurrido en un tratamiento ilícito de datos personales".

"Además, no pueden ser objeto de tratamiento los datos personales obtenidos de una red social o de internet, sin que conrurra alguna de las baes de legitimación previstas en el artículo 6 del RGPD", finaliza.

Por todo ello, la AEPD ha resuelto imponer a Sophie et Voilà una multa de 10.000 euros por la comisión de una infracción muy grave, tal y como recoge el artículo 83.5 de La Ley General de Protección de Datos.

27.09.2022. Multan con 70.000 euros a BBVA por requerir el DNI a una clienta que solicitó el contacto de una sucursal. FUENTE: facua.org

La Agencia Española de Protección de Datos (AEPD) ha impuesto una multa de 70.000 euros al BBVA por requerir una fotocopia del DNI a una mujer interesada en obtener los datos de contacto de una sucursal bancaria con el propósito de llevar a cabo una consulta relativa a los movimientos de su cuenta.

Según recoge Economistjurist.es, la entidad bancaria le remitió a esta clienta un certificado de movimientos donde se le informaba de que, para cualquier tipo de aclaración sobre el mismo, debía dirigirse a una sucursal ubicada en su municipio.

Tras pedir que le facilitasen los datos de contacto de dicha sucursal, le derivaron directamente a un número de teléfono donde le comunicaron que no podían ofrecerle ninguna información por esta vía, instándole a hacer su solicitud a través de correo electrónico al departamento de atención al cliente.

La clienta envió un email, y la respuesta al mismo fue que debía aportar una copia de su DNI para tramitar la consulta. La mujer, al considerar desproporcionada la petición, decidió poner una reclamación ante la Agencia Española de Protección de Datos.

Este organismo entendió que BBVA había vulnerado el artículo 5 del Reglamento General de Protección de Datos (RGPD) al requerir a la reclamante, con el fin de atender su petición, una copia del DNI. Esta norma europea recoge que los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos)".

Por todo ello, la AEPD estableció una sanción de 70.000 euros. El BBVA ha reconocido su responsabilidad y ha pagado voluntariamente la cuantía de 42.000 euros, haciendo uso de las dos reducciones previstas legalmente (reducción del 20% por reconocimiento de responsabilidad y reducción del 20% por pago voluntario).

28.09.2022. La gestión de los datos personales de los currículums: un análisis jurídico. FUENTE: economistjurist.es

La normativa europea y, por ende la española, incluyen vías que tienen como fin último la protección de los datos personales de los ciudadanos. En este contexto, las empresas tienen la obligación de ser especialmente diligentes a la hora de tratar la información de sus clientes y empleados.

Una de las cuestiones relacionadas con la protección de datos que a priori pueden provocar más problemas a las empresas es el tratamiento de la información incluida en los currículums que los candidatos a un puesto de trabajo, bien dentro de un proceso de selección, bien de manera espontánea, envían a las empresas. Hay ocasiones en las que una compañía puede recibir un alud de CV cuando se llevan a cabo procesos de selección, lo cual puede entrañar un reto, ya que un tratamiento inadecuado de los datos puede llegar a suponer importantes multas.

Según explica Isabel Martínez Moriel, socia de Andersen en el área de Privacy, IT & Digital Business, la ley española en cuanto a la protección legal de este derecho está homogeneizada con la de la Unión Europea. En este sentido, explica que “el derecho a la protección de datos es un derecho fundamental reconocido en la Carta de los Derechos Fundamentales de la UE”. “Con carácter adicional”, matiza, “en toda la UE se aplica de forma directa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, general de protección de datos (RGPD) por lo que los derechos y obligaciones relativas al derecho a la protección de datos son los mismos en toda la UE”.

Recuerda Martínez Moriel que en España se aprobó también la Ley Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) que, además de establecer el procedimiento administrativo sancionador (que requería la aprobación de ley orgánica), individualiza y aclara algunas de estas obligaciones.

En este sentido, la socia de Andersen explica, con respecto a la Ley Orgánica, que "a través del Título X, dedicado a la garantía de derechos digitales que afecta directamente a los derechos de los trabajadores, se incluye tanto la jurisprudencia como las aclaraciones necesarias para aplicar las obligaciones del RGPD en el caso de tratamientos de datos de empleados en el ámbito digital y el derecho a la desconexión digital".

Con la ley en la mano, ¿qué tienen que hacer las empresas para gestionar los datos personales de los CV? Alejandro Padín, socio del Departamento Mercantil de Garrigues, asegura que "en realidad no hay ningún problema, ya que aplica la regla general de que cualquier empresa que trate datos personales tiene que informar al interesado". "Si una empresa recibe un CV y lo incorpora a algún proceso, o lo conserva para futuros procesos, se encuentra tratando datos personales de los candidatos y, por tanto, debe cumplir con las exigencias de la normativa aplicable", señala.

Entre las cuestiones que tienen que tener en cuenta las compañías está "tratar esos datos de forma lícita, informar a los interesados sobre el tratamiento de sus datos, garantizar que los datos solo se usen para los fines que motivaron su recogida (en este caso, gestionar el proceso de selección), tienen que mantenerlos actualizados en la medida de lo posible, conservarlos solo durante el tiempo necesario para gestionar su candidatura y, por supuesto, debe mantener dichos datos seguros y protegidos ante cualquier acceso no autorizado".

Por su parte, Antonio Benitez Ostos, socio director de Administrativando, señala que "para que las empresas puedan tratar los datos de los candidatos tienen que tener su consentimiento". En este sentido, recuerda que "en los grandes portales de empleo este consentimiento se da cuando son aceptadas las condiciones generales", en las que se incluye información sobre cómo van a ser tratados los datos.

CV enviados al margen de procesos de selección

Hay un elemento que puede estar marcado por la controversia y es los casos en que las empresas reciben CV al margen de procesos de selección. Los remitentes de estos currículums tienen que ser informados del tratamiento que se va a dar a sus datos por parte de la empresa que recibe los mismos. De lo contrario, la empresa se puede enfrentar a una multa de la Agencia Española de Protección de Datos (AEPD).

Alejandro Padín explica que "es cierto que el RGPD supuso un cambio de paradigma en cuanto a la forma entender el cumplimiento a través del principio de accountability que, entre otros, transfiere a los responsables del tratamiento de datos la obligación no solo de cumplir con la normativa, sino también de poder demostrar dicho cumplimiento".

Teniendo esto en cuenta, "aunque la norma sí recoja ciertos requisitos formales, son las propias empresas las que deben valorar cuál es la mejor opción para garantizar la protección de los datos que se encuentran bajo su responsabilidad. Por lo tanto, las

compañías que reciban CV, además de cumplir con los requisitos formales que exige la norma, deberán implantar todas las medidas técnicas y organizativas necesarias para poder tratar los datos adecuadamente", destaca el socio de Garrigues.

La cuestión es que, según explica Antonio Jesús Pérez Valderrama, director de Administrativando, "para que una empresa pueda evaluar un currículum tiene que tener el consentimiento del remitente". Esto significa que la firma debe remitir un modelo de consentimiento expreso para que lo firme la persona que ha enviado el CV antes de poder analizarlo.

Pérez Valderrama asegura que, "este proceso no es muy operativo" ya que "la obligación se invierte porque no se obliga a dar el consentimiento previo", sino que hay que pedirlo a posteriori. Entiende este abogado que "esta obligación puede ser una pesadilla para la empresa" porque "un Departamento de Recursos Humanos que reciba 20 currículums al día necesita a una persona solo para gestionar las respuestas". Además, recuerda que la empresa tiene la obligación de destruir el CV de las personas que no han dado su consentimiento.

Por su parte, Isabel Martínez destaca que "el RGPD y la LOPDGDD protegen adecuadamente a los ciudadanos que envían sus datos a empresas". Pone como ejemplo que la AEPD, en su Resolución PS/00237/2021, ha recordado la obligación de las empresas de informar adecuadamente a los titulares de los datos, en este caso a un aspirante a un puesto de trabajo, del tratamiento de datos personales que se va a realizar con los datos de su CV, con independencia de que este aspirante haya enviado de forma proactiva su CV a dicha empresa.

En este caso, la AEPD señaló que "la entidad reclamada no le ha facilitado información relativa al tratamiento que efectuarían con sus datos personales ni de la posibilidad de ejercitar los derechos ante el responsable del tratamiento". Por ello, "es importante recordar que las empresas, para evitar este tipo de riesgos, deben diseñar procedimientos internos que les permitan cumplir con el RGPD, así como generar evidencias de su cumplimiento y diligencia" manifiesta la socia de Andersen.

Aun cuando la protección de los ciudadanos puede estar afianzada, hay un aspecto que no ha sido recogido en la normativa: el tiempo que las empresas pueden tener la información recogida en los currículums. Antonio Benitez Ostos relata que, aunque no existe un tiempo fijado en la norma, por lo general "se ha establecido un plazo de entre un año y medio y dos años para que la empresa conserve la información". A este respecto, señala que sería conveniente que se incluyera el alcance del uso de los datos en las condiciones firmadas por los ciudadanos.

A juicio del socio director de Administrativando, "salvo que se haya firmado un consentimiento amplio que permita guardar los datos una vez terminados los procesos de selección, la empresa debería eliminar los datos cuando el motivo del almacenamiento expira". Aquí el "debería" cobra importancia, ya que, según explica Benitez Ostos, la empresa, al no estar obligada por la ley, puede mantener los CV el tiempo que quiera, salvo que los ciudadanos decidan revocar la autorización a través de los canales de los

que la empresa debe disponer a tal efecto o a través del responsable de protección de datos.

Datos de las redes sociales

Un aspecto en el que las empresas tienen que ser especialmente cuidadosas es el del uso datos difundidos por los usuarios de Internet a través de plataformas o redes sociales como Linkedin. Alejandro Padín recuerda que "para realizar un tratamiento de datos personales siempre se debe contar con una base de legitimación de las previstas en el artículo 6 del RGPD. El hecho de que un dato personal sea público no quiere decir que un tercero pueda utilizarlo para otros fines distintos de los que tenía el interesado con su publicación". En este sentido, "la subida de datos personales que un usuario hace en una red social tiene como finalidad la que haya previsto el usuario para dicha publicación en esa red y, en general, compartir la información que el usuario desee con el resto de esa comunidad. Pero lo anterior no legitima el uso de sus datos para llevar a cabo cualquier otra operación con ellos".

Sobre esta cuestión, Isabel Martínez aclara que "se ha de distinguir, en todo caso, entre el acceso a un perfil de candidatos que ha contestado a una oferta de trabajo publicada por Linkedin, del acceso al perfil público de un candidato que ha optado a una oferta de trabajo o que ha enviado una candidatura espontánea por otro medio".

"En el primer caso, la empresa puede acceder y tratar los datos personales del candidato que aparecen en el LinkedIn pues es el candidato el que ha optado por esa oferta en la misma red", manifiesta la socia de Andersen.

"En el segundo caso", asegura Isabel Martínez, "la AEDP ha aclarado que si bien, materialmente, el seleccionador puede acceder al perfil público de un candidato en las redes sociales, el seleccionador/empleador no puede efectuar un tratamiento de los datos obtenidos por esta vía si no cuenta para ello con una base jurídica válida". La propia AEPD matiza que "la indagación en los perfiles de redes sociales de las personas candidatas a un empleo sólo se justifica si están relacionados con fines profesionales. El tratamiento de los datos obtenidos por esta vía únicamente será posible cuando se demuestre que dicho tratamiento es necesario y pertinente para desempeñar el trabajo. Y la persona trabajadora tiene derecho a ser informada sobre ese tratamiento".

Al margen de la cuestión de la protección de datos, el uso de información de las redes sociales de una persona tiene una variable jurídico-laboral importante que explica Cecilia Pérez, socia del Departamento Laboral de Garrigues. Entiende que "las empresas deben ser muy cautelosas con la información que toman en consideración para tomar sus decisiones de contratación o no de una persona".

Argumenta Cecilia Pérez que "la información que una persona comparte en redes sociales debería ser veraz y precisa, pero podría no serlo. Si no lo fuera, y la empresa contrata a la persona basándose en información no veraz no facilitada directamente por esta, y más tarde la empresa descubriera que no lo era, podría ser complicado emprender cualquier acción disciplinaria contra la persona, porque sería cuestionable que la persona tuviera un ánimo de engañar a una empresa concreta, para conseguir un trabajo concreto, para el que

se requiriera una determinada experiencia o formación que la persona hubiera dicho públicamente en redes sociales sin facilitar la información a la empresa".

Agencias de colocación
En este análisis sobre el tratamiento de los datos de los CV de los candidatos a un puesto de trabajo no hay que perder de vista el papel que juegan las empresas y agencias de colocación que son contratadas por otras compañías para realizar un determinado proceso de selección.

Para Isabel Martinez, "las empresas o agencias de colocación que apliquen procedimientos adecuados al RGPD para aproximarse a candidatos a través de redes sociales, o publiquen adecuadamente ofertas de trabajo a través de estos medios, cumplirían sus obligaciones legales". A su juicio, "asegurarse del tratamiento de los datos con una base legítima válida siempre, así como de informar de forma adecuada del tratamiento de sus datos personales, finalidades, periodos de conservación y ejercicio de derechos, entre otros, a los candidatos".

Sobre este particular puede surgir una duda. En el caso de que haya un mal uso de los datos aportados por una persona candidata, ¿a quién habría que pedir cuentas, a la agencia o a la empresa que la contrata?

"Pueden darse distintos escenarios", afirma Alejandro Padín, para quien la solución dependerá, entre otras cuestiones, "de las funciones de dichas agencias, de si están actuando sobre su propia base de datos o han recabado datos específicamente para un proceso concreto en una empresa, del momento en que se haya producido la incidencia y del tipo de incidencia y perjuicios causados a los interesados".

La casuística varía en función del papel desempeñado por las agencias de colocación. Así, Padín utiliza el ejemplo de una compañía de colocación contratada por otra empresa para que realice un proceso de búsqueda de un perfil en concreto; en este caso ", la empresa cliente sería la responsable del tratamiento y de cumplir todas las obligaciones legales, mientras que la agencia sería un prestador de servicio y actuaría como encargado del tratamiento".

En otros casos, la agencia podría dedicarse a presentar candidatos de una base de datos propia para distintos procesos de selección que publiquen otras empresas. En este supuesto, "la responsable del tratamiento es la agencia", afirma el socio de Garrigues.

Sea como fuere, Alejandro Padín subraya que "lo más importante para el interesado es que tiene que haber sido informado debidamente del tratamiento de sus datos para el proceso de selección y de las vías para poder ejercitar los derechos de protección de datos que la normativa recoge, sabiendo a quién y cómo debe dirigirse, en caso de cualquier incidencia".

29.09.2022. Finalización del período para la adaptación de los contratos que utilicen las garantías de las cláusulas contractuales tipo de la Comisión Europea para la transferencia internacional de datos. FUENTE: aepd.es

El 7 de junio de 2021 se publicó la Decisión de la Comisión Europea 2021/914, relativa al nuevo conjunto de cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento General de Protección de Datos. Además de sustituir a sus predecesoras, ofrecen garantías para las transferencias entre responsables, entre responsable y encargado, entre encargados y entre encargado y responsable.

Conforme a dicha Decisión 2021/914, las cláusulas contractuales de las Decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE quedaron derogadas a partir del 27 de septiembre de 2021. No obstante, los contratos celebrados antes de dicha fecha con arreglo a las cláusulas de las Decisiones derogadas gozan de un período transitorio de validez de 15 meses, siempre que las operaciones de tratamiento permanezcan inalteradas y las cláusulas contractuales garanticen que la transferencia de datos personales está sujeta a garantías adecuadas.

El periodo transitorio finaliza el próximo 27 de diciembre de 2022, fecha en la que ya no resultarán válidos los contratos celebrados con arreglo a las cláusulas de las Decisiones derogadas, debiéndose proceder a su adaptación a las nuevas cláusulas contractuales tipo aprobadas por la Decisión 2021/914 de la Comisión Europea.

OCTUBRE

10/10/2022. Instalación de cámaras en comunidades de propietarios. FUENTE: laregion.es

La instalación de videocámaras por las comunidades de propietarios, está siendo cada vez, más habitual, lo cual, supone el tratamiento del dato personal por antonomasia, la imagen.

Las grabaciones de personas, están sujetas a una serie de requisitos y obligaciones que se deben de respetar y cumplir y, a tal fin, la Agencia Española de Protección de Datos (AEPD) ha publicado una ficha práctica para la instalación de cámaras en las comunidades de propietarios, la cual recoge que:

Para la instalación de cámaras en zonas comunes será necesario el acuerdo de la Junta de Propietarios que cuente con el voto favorable de las 3/5 partes de la totalidad de los propietarios que a su vez representen las 3/5 partes de las cuotas de participación tal y como desarrolla el artículo 17.1 de la Ley de Propiedad Horizontal.
Se recomienda que en el acuerdo se reflejen algunas de las características del sistema de videovigilancia, como el número de cámaras o el espacio captado por las mismas.

Previamente a su puesta en funcionamiento, se elaborará un registro de actividades referido a este tratamiento.

Se instalarán en los distintos accesos a la zona videovigilada, y en lugar visible, uno o varios carteles que informen de que se accede a una zona videovigilada. El cartel indicará de forma clara la identidad del responsable de la instalación ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos, y dónde obtener más información sobre el tratamiento de los datos personales.
Las cámaras solamente podrán captar imágenes de las zonas comunes de la comunidad. No podrán captarse imágenes de la vía pública salvo que resulte imprescindible para la finalidad perseguida, a excepción de una franja mínima de los accesos al inmueble, ni tampoco imágenes de terrenos y viviendas colindantes o de cualquier otro espacio ajeno.
La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero no exime a la comunidad de propietarios del cumplimiento de la normativa en materia de protección de datos personales.
El acceso a las imágenes estará restringido a las personas designadas por la comunidad. En ningún caso estarán accesibles a los vecinos mediante canal de televisión comunitaria.
Si el acceso se realiza con conexión a Internet se restringirá con un código de usuario y una contraseña (o cualquier otro medio que garantice la identificación y autenticación unívoca), que sólo serán conocidos por las personas autorizadas a acceder a dichas imágenes.
El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido. A las imágenes grabadas accederá sólo el personal autorizado que deberá introducir un código de usuario y una contraseña.
Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación, transcurrido el cual se procederá al borrado, salvo que se utilicen las imágenes para denunciar delitos o infracciones se acompañarán a la denuncia y serán conservadas para su posible entrega a las Fuerzas y Cuerpos de Seguridad o a los Juzgados y Tribunales que las requieran. No podrán utilizarse para otro fin.
La petición de imágenes por las Fuerzas y Cuerpos de Seguridad se realizará en el marco de actuaciones judiciales o policiales. El requerimiento al responsable del tratamiento será el documento que ampare a éste para ceder datos a las mismas o a los Juzgados y Tribunales que los requieran. Es decir, debe de requerirlo por escrito.

21/10/2022. El Constitucional avala el despido de un trabajador grabado sin previo aviso por la empresa mientras robaba productos. FUENTE: 20minutos.es

El Tribunal Constitucional ha avalado el despido de un trabajador que fue grabado sin previo aviso por la empresa. El hombre perdió su empleo después de que el gerente observara que el empleado guardaba productos de la compañía en una bolsa de la competencia para, supuestamente, venderlos a terceras personas, según recoge EFE.

Para confirmar sus sospechas, al día siguiente el encargado revisó las grabaciones de las cámaras de seguridad instaladas en la empresa. Al ver que efectivamente el empleado había robado algunos productos, procedió a rescindir su contrato.

Los empleados no habían sido avisados previamente de que el material recogido por las cámaras podía ser usado en su contra en caso de supuestas irregularidades.

Despido improcedente

En un primer momento, el despido fue avalado por un juzgado de lo Social de Vitoria-Gastéiz, pero el trabajador recurrió ante el Tribunal Superior de Justifica del País Vasco. La sentencia le dio la razón, asegurando que se trataba de un despido improcedente.

El Tribunal Superior alegó que las pruebas aportadas por la empresa eran ilícitas porque, según recoge el artículo 12 del Reglamento (UE) 2016/679, el uso de cámaras de seguridad para el control exige informar previamente a los empleados "de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo".

La ley de protección de datos recoge que la empresa debe advertir a los trabajadores -ya sea de forma individual o a través del comité- de la posibilidad de utilizar las imágenes obtenidas por sus sistemas de seguridad para controlarlos.

Desacuerdo en el Constitucional
Tras el fallo del Tribunal Superior, la empresa decidió acudir al Supremo, pero este inadmitió el recurso por falta de contradicciones entre las sentencias anteriores.

Ante esta respuesta negativa, la empresa afectada planteó un recurso de amparo en el Constitucional, considerando que se había vulnerado su derecho a la tutela judicial efectivo por rechazarse como prueba la grabación que incriminaba al empleado.

La mayoría conservadora del tribunal le ha dado la razón, tras un debate que se saldó por 6 votos a 5. El Constitucional ha considerado que la prueba de la grabación es lícita porque en la entrada de la empresa había un cartel informando de la existencia de cámaras.

La sentencia del Pleno valida la grabación al recordar que "la instalación del sistema de videovigilancia estaba advertida en un lugar visible de la empresa, mediante un distintivo que se ajustaba a la normativa vigente sobre protección de datos" y señalar que este hecho era conocido por los trabajadores por un precedente en 2014 de un empleado que fue despedido "por la constatación de una conducta ilegal mediante la utilización de las imágenes captadas".

Y añade que "no tendría sentido que la instalación de un sistema de seguridad en la empresa pudiera ser útil para verificar la comisión de infracciones por parte de terceros y, sin embargo, no pudiera utilizarse para la detección y sanción de conductas ilícitas cometidas en el seno de la propia empresa".

Los progresistas, por su parte, votaron en contra de la empresa amparándose en la mencionada ley de protección de datos. Además, han argumentado que, aunque la legislación permite emplear las imágenes en caso de delito, consideran que en este caso no se ha dado la circunstancia porque el repaso de las grabaciones se produjo al día siguiente basándose en una sospecha del gerente.

Videovigilancia de los trabajadores
Los empresarios pueden grabar a sus trabajadores en el desarrollo de sus funciones dentro de la empresa. Así lo recoge el Estatuto de los Trabajadores en su artículo 20.3: "El empresario podrá adoptar las medidas que estime más oportunidad de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales".

La empresa no necesita una autorización por parte de los trabajadores. Únicamente está obligado a informar de forma clara de la colocación y la finalidad de las mismas. Las cámaras están obligadas a respetar el derecho a la intimidad de los trabajadores, por lo que no podrán instalarse en vestuarios, comedores, aseos, zonas de descanso ni en la vía pública, según recoge la Agencia Española de Protección de Datos.

La videovigilancia ha de tener como único fin preservar la seguridad de las personas y de los bienes del negocio.

26/10/2022. Protección de Datos sanciona a la Comunidad de Madrid por dejar al descubierto datos personales de pacientes. FUENTE: eldiario.es

La Agencia Española de Protección de Datos ha sancionado a la Consejería de Sanidad de la Comunidad de Madrid por una brecha de seguridad que dejó al descubierto datos personales de ciudadanos a través de su sistema de autocita para la vacunación contra la COVID-19, que abrió el 24 de mayo de 2021. El fallo estuvo activo desde ese día hasta el jueves 10 de junio, tras el aviso de elDiario.es.

La Consejería admitió entonces el fallo, pero trató de restarle importancia, alegando que ningún "actor malicioso" había accedido a los datos de los residentes en la región porque, de haber sucedido, "el Centro de operaciones de ciberseguridad que monitoriza los sistemas de información ininterrumpidamente, lo hubiera detectado". No obstante, Facua Madrid puso los hechos en conocimiento del organismo público encargado de velar por la protección de datos en España.

Ahora, la Agencia ha dado la razón a la asociación de consumidores, en una decisión contra la que cabe recurso, al considerar que la Consejería vulneró hasta cuatro artículos del reglamento en este incidente. Por ello, le impone una sanción de apercibimiento, y no económica, la fórmula prevista para las instituciones de las comunidades autónomas en la Ley de Protección de Datos Personales y garantía de los derechos digitales.

Durante el incidente, la página web del sistema de citas para la vacunación dejaba a la vista el nombre completo, DNI, número de teléfono, fecha de nacimiento y los números de identificación sanitaria, tanto autonómicos como nacionales de cualquier ciudadano al solicitar una cita con su Código de Identificación Personal de la Comunidad de Madrid. Como confirma ahora la Agencia, estos datos quedaban al descubierto al introducir el DNI de las personas, aunque fuera al azar.

El 5 de octubre de 2021, la inspección solicitó a la Consejería de Sanidad madrileña información relativa de los hechos ocurridos, sus causas, el número de personas afectadas y las posibles consecuencias para las víctimas de esta brecha de seguridad, así como el motivo por el que no se notificó el incidente en el plazo previsto de 72 horas. Una solicitud que se reiteró, según el escrito, el 1 de diciembre de aquel año, tras no obtener respuesta por parte de la administración regional.

El 14 de marzo, todavía sin respuesta, la dirección de la Agencia acordó iniciar un procedimiento sancionador contra la Consejería que dirige Enrique Ruíz Escudero. Tras analizar los hechos, este organismo concluye que "el fallo detectado relacionado con este

sistema de información se debe a una exposición de información de datos personales (públicos) accedidos mediante una cookie de sesión válida, y editando la url accedida uno de los cambios de entrada llamado "idPaciente" con un DNI válido". Esto permitía "visualizar una serie de datos personales correspondientes a la persona con el DNI utilizado", algo que se debía a que la aplicación web "contaba con mecanismos de bloque insuficientes".

Según el documento al que ha tenido acceso elDiario.es, "con fecha de 15 de julio de 2022, la directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador" a la Consejería, por varias infracciones del Reglamento General de Protección de Datos. La administración se justificó alegando que en los meses de mayo y junio de 2021, cuando se produjo el incidente, se encontraba "en un momento muy crítico relacionado con la gestión de la pandemia".

La Agencia ha considerado no informar a la Autoridad de Control, debido "al nivel de riesgo de la incidencia" y "teniendo en cuenta el bajo volumen de datos que podrían haberse afectado, la tipología de los mismos, siendo únicamente datos de carácter identificativo" así como que el impacto provocado en los interesados fue "inexistente". Sin embargo, critica que "no se ha presentado por parte de la Consejería una valoración de riesgos realmente efectuada".

27/10/2022. Nueva multa de Protección de Datos a BBVA: 70.000 euros por filtrar la dirección personal de un abogado a un cliente. FUENTE: confilegal.com

La Agencia Española de Protección de Datos ha vuelto a sancionar al BBVA. En esta ocasión, tendrá que abonar una multa de 70.000 euros por entregar un documento a una clienta en el que aparecía el domicilio particular de su abogado (cliente del banco).

En noviembre de 2020, el reclamante, en condición de abogado, presentó en nombre de su clienta una reclamación ante la entidad bancaria. Una semana después, BBVA entregó en mano a dicha clienta un escrito relativo a la reclamación y, en el documento, constaba el domicilio particular del letrado en vez del despacho profesional.

El letrado consideró que el banco había revelado su domicilio particular, que no era conocido por su clienta y que fue facilitado por BBVA. Pues él era cliente de la entidad al abrir una cuenta bancaria con ellos, por lo que el banco disponía de sus datos personales. Por estos hechos, interpuso una reclamación contra el banco solicitando una indemnización por los hechos ocurridos.

Como prueba, presentó la reclamación que puso en calidad de abogado en nombre de su clienta en la que no se indica ninguna dirección de contacto. Así como el escrito del BBVA en el que se disculpa e indica que han puesto los hechos en conocimiento de los responsables indicados con el objetivo de adoptar medidas y eliminar cualquier riesgo de reincidencia.

EL DIRECTOR DE LA OFICINA DESCONOCÍA QUE EN EL PAPEL APARECIESE EL DOMICILIO PARTICULAR DEL LETRADO

El banco alegó que tras analizar los hechos se constató que la incidencia tuvo lugar por un error puntual e involuntario y que fue reparado de forma inmediata cuando tuvo conocimiento de ello. Pues el director de la oficina desconocía que se trataba de la dirección particular y, por lo tanto, un dato personal del representante.

En cambio, la AEPD manifestó que la entidad no explicó en qué consistió el error alegado. Pero, aun así, "no puede admitirse que la actuación de la entidad derive de un error" ya que pasar pasarlo por alto sería ignorar la aplicación del Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)

Según la reclamación de la AEPD, este hecho pone de manifiesto que "la entidad reclamada no ha adoptado de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar la seguridad y confidencialidad de los datos de sus clientes. Especialmente, las dirigidas a impedir el acceso a la información por terceros no autorizados, como de hecho ocurrió cuando la propia entidad reclamada facilitó al cliente de la parte reclamante el documento de acuse de recibo de la reclamación formulada, dirigido a la parte reclamante y a su domicilio personal".

Por ello, ha multado al banco con 70.000 euros. En concreto, 25.000 euros por la infracción del artículo 5.1.b) del RGPD; 20.000 euros por la infracción del artículo 32 del RGPD y 25.000 euros por la infracción del artículo 5.1.f) del RGPD.

Pero no es la primera vez que BBVA recibe una sanción por protección de datos. En junio de 2022, tuvo que enfrentarse a una multa de 48.000 euros por desvelar a un tercero el saldo de la cuenta de una clienta.

En agosto de 2021, fue multado con 200.000 euros por facilitar, a través del sistema de atención telefónica automatizado, información asociada a un DNI con tan solo facilitar su número

Por otro lado, En 2020, tuvo que pagar 5 millones de euros por infringir varios puntos del RGPD al enviar publicidad a personas que ejercían el derecho de oposición a la cesión de datos con fines promocionales.

28/10/2022. Telefónica ha sufrido un ciberataque: si eres cliente de Movistar u O2, así puedes cambiar la contraseña. FUENTE: xataka.com

Telefónica ha detectado una brecha de seguridad en sus sistemas y está avisando a sus clientes. Hace unas semanas sufrió un ciberataque y ahora ha tomado la decisión de alertar de este hecho a los distintos usuarios, tanto de Movistar como de O2.

La operadora explica que se han tomado las medidas necesarias y confirma que no está afectado ningún dato personal sensible que pueda identificarnos, pero sí puede estar en riesgo información técnica sobre nuestros equipos y nuestro WiFi.

Si eres cliente de Telefónica, revisa tu WiFi

En un correo enviado a los usuarios, Movistar explica que este acceso no autorizado puede afectar a los equipos asociados a nuestro número de teléfono, desde el router hasta el decodificador del televisor o el amplificador WiFi.

En concreto parece estar en riesgo el identificador único (la MAC), detalles sobre el fabricante del equipo, configuración de los puertos de la conexión, el nombre de la WiFi y la contraseña. Precisamente por esto, la operadora recomienda a todos los usuarios que cambien la contraseña por seguridad, ya que al estar comprometidos estos datos es más fácil que un posible atacante logre acceder a nuestro WiFi.

En el comunicado, la operadora explica que "los datos sustraídos no pueden explotarse de manera remota, la única manera de usarlos es estando físicamente en el rango de acceso de tu WiFi".

De igual manera, como exigen las leyes de privacidad, Telefónica pone a disposición de los usuarios el contacto de su delegado de Protección de Datos para cualquier incidencia o consulta.

Cómo cambiar la contraseña del WiFi
Si eres cliente, desde aquí recomendamos encarecidamente cambiar la contraseña del WiFi. Para hacerlo deberemos acceder a la configuración del router. Esto puede hacerse accediendo desde cualquier navegador a la dirección IP por defecto.

Para ello hay que escribir la dirección 192.168.1.1 en la barra de direcciones (http://192.168.1.1). Si no, funciona, prueba con la 192.168.0.1. Una vez dentro accederemos al panel del router, donde deberemos escribir el nombre de usuario y contraseña.

Desde el apartado de Mi Movistar podremos acceder a los ajustes, ahí la opción de "Cambio contraseña del router" o "WiFi / Contraseña". Una vez dentro deberemos añadir una contraseña alfanumérica de al menos ocho caracteres. Desde hace años Telefónica dispone del Portal Alejandra, una base web donde configurar el router de forma sencilla.

A este portal deberemos acceder para cambiar la contraseña de nuestra WiFi y estar más seguros. Una medida de seguridad que deberíamos hacer cada cierto tiempo y que toma más relevancia en casos de ciberataque.

NOVIEMBRE

03/11/2022. 10.000 euros de multa al despacho Ackermann & Schwartz por tratar un currículum sin consentimiento del titular. FUENTE: confilegal.com

La Agencia Española de Protección de Datos (AEPD) ha multado con 10.000 euros al despacho **Ackermann & Schwartz Attorneys At Law,** titular de la página www.madridlaw.es por infringir dos artículos del Reglamento General de Protección de Datos, el 6.1 y el 13.

Según la AEPD, el bufete obtuvo datos personales de los usuarios de la página web sin previo consentimiento y, además, en el apartado de "Política y Privacidad", la información era de difícil acceso, insuficiente y en inglés.
La reclamante es una abogada que se quiso postular a un puesto de trabajo que vio en una página web. Tras enviar el CV, recibió una llamada de una persona para realizarle una entrevista, pero, según explicó, no le informó del nombre de la empresa que estaba ofreciendo el puesto.

El día de la entrevista, el encargado de hablar con ella entró a la sala con su currículum impreso, pero, según la reclamación interpuesta, **la empresa no le advirtió en ningún momento del tratamiento que se le iba a dar a sus datos personales.**

Asimismo, según la reclamación, la abogada supo a qué empresa estaba postulando porque vio que en la oficina había pegatinas con el logotipo de Ackermann & Schwartz. A ello añadió que, en la web corporativa de la empresa -citada anteriormente- no constaba ninguna información relativa al Reglamento General de Protección de Datos ni se identificaba a la empresa titular de la página.

INFORMACIÓN «INSUFICIENTE» Y EN INGLÉS
La Subdirección General de Inspección de Datos procedió a realizar las investigaciones pertinentes para esclarecer los hechos en cuestión. Según se constató, la empresa podía obtener datos personales de los usuarios a través de un formulario donde se podía introducir el nombre, el correo electrónico, el asunto y se podía dar la opción de enviar. **Los usuarios no consentían que se tratasen sus datos.**

Por otro lado, en el apartado de "Política de Privacidad", la web señalaba que la información personal que se facilitase se incorporará a un fichero de datos de carácter personal con titularidad de Ackermann & Schwartz y que, las finalidades del tratamiento de datos, serían para gestionar y tramitar las solicitudes realizadas.

En cambio, según la AEPD, la información suministrada en dicho apartado **es "totalmente insuficiente".** Pues carece, por ejemplo, de la identidad y los datos de contacto del responsable; los datos de contacto del delegado de protección de datos o, en su caso, los destinatarios de los datos personales y de la información necesaria para ejercitar los derechos que asisten los usuarios, cómo y dónde ejercitarlos. Además, está en inglés.

La AEPD, en su resolución, ha explicado que cuando el tratamiento de los datos personales se realiza a través de un sitio web, la "Política de Privacidad" es el documento mediante el cual el titular de la web debe informar sus clientes y usuarios sobre la gestión que realizará de los datos personales que se recopilarán al navegar en el sitio.

«SE DEBE PROPORCIONAR UN ACCESO FÁCIL Y DIRECTO»

Por tanto, antes de que el usuario facilite sus datos personales y dé su consentimiento al tratamiento de estos, **se le debe facilitar un acceso simple y directo a la "Política de Privacidad" de la web.**

Respecto a la forma de obtener el consentimiento del interesado, continúa la AEPD, la solicitud debe ser realizada a través de un **acto afirmativo claro y voluntario, facilitando una casilla en blanco,** o un mecanismo similar, donde el usuario deba marcar o cliquear de forma explícita la aceptación de la "Política de Privacidad", mediante fórmulas como: «*He leído y acepto las condiciones de la política de privacidad* o equivalentes.

Por ello, ha sancionado con **5.000 euros al despacho por la infracción del artículo 6.1 RGPD,** al poder obtener datos personales de los usuarios de la página web sin haber obtenido previamente su consentimiento para el tratamiento de estos.

Y, por otro lado, otros **5.000 por infracción del artículo 13 RGPD,** al proporcionar, en la "Política de Privacidad" de la página web, información en un idioma no oficial en España por proporcionar información insuficiente.

09/11/2022. Multa de 70.000 euros a UPS por entregar un paquete a un vecino sin autorización del destinatario. FUENTE: elmundo.es

La Agencia Española de Protección de Datos sanciona a la empresa de mensajería al entender que se han cedido sus datos personales a un tercero sin su consentimiento.

La habitual práctica de recoger los paquetes que le envían a un vecino puede tener los días contados. **La Agencia Española de Protección de Datos (AEPD) ha impuesto una multa de 70.000 euros a la empresa de mensajería UPS** por entregar un pedido realizado por Internet a la empresa Media Markt a un vecino del destinatario sin su autorización.

Los hechos se remontan a marzo de 2021, cuando la persona que realizó la compra denunció que al dejarle el envío a otra persona **se han cedido sus datos personales a un tercero, sin su consentimiento**.

Y así lo ha entendido la agencia, que considera que se han vulnerado **el precepto 5.1 f) del Reglamento General de Protección de Datos (RGPD) y el artículo 32 del RGPD "al violar el principio de integridad y confidencialidad**, así como no adoptar las medidas de seguridad necesarias para garantizar la protección de los datos de carácter personal de sus clientes", según recoge la resolución. Por el primero **impone a UPS una multa de 50.000 euros y por segundo 20.000**.

RECLAMACIÓN INICIAL A MEDIA MARKT
Aunque el usuario reclamó inicialmente a Media Markt, **la AEPD considera que es United Parcel Service (UPS) la responsable de garantizar la protección de los datos del cliente**.

Más en El Mundo
La resolución tiene en cuenta que, en el contrato entre ambas empresas, UPS especifica que "si el receptor no se encuentra disponible, **el paquete podrá ser depositado en el buzón de correspondencia postal del domicilio del receptor, si se considera**

apropiado, o entregado al vecino salvo que el remitente haya excluido esta opción de entrega mediante la elección del servicio adicional aplicable".

Sin embargo, para la Agencia Española de Protección de Datos, **aunque Media Markt no haya notificado nada en ese sentido a UPS, el transportista no puede proporcionar los datos personales a un tercero y por ese motivo le impone la multa**. La empresa de mensajería puede recurrir la resolución ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

DICIEMBRE

02/12/2022. Esta es la multa que le puede caer a tu empresa si te molesta fuera de tu jornada. FUENTE: economiadigital.es

Las nuevas tecnologías están cada vez más presentes en nuestras vidas. También en la laboral. Si bien facilitan y agilizan gran parte de las tareas asociadas a los puestos de trabajo, su uso también conlleva una serie de inconvenientes. Y es que, puede favorecer que **el empleado esté conectado más horas de las que le corresponde**, revisando correos o contestando mensajes de WhatsApp, por ejemplo.

Precisamente, en este contexto, es donde adquiere más importancia la **desconexión digital.** Se trata de un derecho que poseen los empleados y que les brinda libertad para no tener que conectarse a ningún dispositivo ni programa corporativo fuera de su jornada de trabajo, pero también a lo largo de sus vacaciones o días de descanso.

Derecho a la desconexión digital
Cabe destacar que todos los aspectos relacionados con la desconexión digital están regulados la **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y Garantías de los Derechos Digitales**. En concreto, el artículo 88 deja bien claro que tanto los trabajadores como los empleados públicos «tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, **el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal familiar**".

«Las modalidades de ejercicio de este derecho **atenderán a la naturaleza y objeto de la relación laboral**, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores», aclara la normativa.

Asimismo, concreta que el empleador habrá de elaborar una **«política interna»** dirigida a la plantilla de empleados, pero también a las personas que ocupen puestos directivos. En el documento, se deberán definir las «modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática».

En esta línea, se especifica que se habrá de preservar el derecho a la desconexión digital en **«los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas».**

Sanción

Pero, **¿qué ocurre cuando la empresa incumple la normativa?** «Las empresas no pueden obligar ni forzar a que la persona trabajadora, fuera del horario laboral, esté constantemente **hiperconectada** o pendiente del correo electrónico, WhatsApp, chat o llamadas telefónicas de la empresa o relacionadas con ella».

Tal y como recoge la **Ley de Infracciones y Sanciones del Orden Social (LISOS),** las irregularidades en el derecho a la desconexión digital de los empleados se consideran infracciones graves y, consecuentemente, la multa interpuesta puede oscilar **entre los 751 y los 7.500 euros.**

El hecho de no contar con un código empresarial que regule la desconexión digital, según alerta San José, puede desembocar en una **«hiperconectividad laboral»** que, a su vez, puede provocar «en algunos trabajadores estrés, fatiga, síndrome del trabajador desgastado o una violencia laboral como el ciberacoso o también denominado 'network mobbing', afectando totalmente a su salud».

Por ello, la sanción para los casos vinculados al acoso o ciberacoso puede ascender hasta los **225.018 euros**.

24/12/2022. Multa de 16.000 euros al Hospital Recoletas de Ponferrada por premarcar un formulario de protección de datos. FUENTE: confilegal.com

La Agencia Española de Protección de Datos (AEPD) ha multado con **20.000 euros - 16.000** por acogerse a la reducción por pago voluntario- al Hospital Recoletas Ponferrada por premarcar en una tablet casillas relacionadas con la protección de datos que los pacientes tenían que rellenar antes de ser atendidos.

Según la resolución a la que ha tenido acceso Confilegal, una usuaria presentó una reclamación ante la AEPD porque a finales de diciembre de 2021 acudió a la Clínica Recoletas a que le realizaran unos análisis.
Cuando llegó su turno enseñó el volante y le pidieron la tarjeta del seguro para gestionar el servicio. Tras esto, le dieron una tablet y le dijeron que tenía que firmar un documento de protección de datos **para poder procesar la información.**

Tras coger el dispositivo electrónico se puso a leerlo y le dijo a la empleada que no estaba de acuerdo con los puntos 2 y 3 del formulario que ya estaban marcados y que estaban relacionados con **compartir su información con empresas terceras y recibir propaganda.**

La empleada de la clínica le dijo que entonces no podían atenderle ya que, sin su firma, no se podía gestionar nada. La usuaria le recordó que ella no se negaba a firmar el documento, sino sólo los ítems marcados por ellas.

"Entonces ella hizo algo en la tablet y me la devolvió y en ese momento aparecían desbloqueados los ítems", relató en la reclamación. Por lo que pudo marcar las casillas que consideraba oportunas y firmó. Asimismo, no le enviaron una copia del documento.
Tras hacerse los análisis **pidió hablar con el gerente** para hacerle constar su malestar, pero al no estar presente, le ofrecieron poner una reclamación asegurándola que esa misma semana le llamaría. Cuando pudo hablar con la gerente le pidió disculpas y aseguró haber hablado con la responsable y ésta le explicó que "siempre rellenaban los datos porque la gente era mayor".

«ES ALGO QUE NUNCA DEBIÓ SUCEDER»
La gerente le reconoció a la usuaria reclamante que, efectivamente, **está práctica era ilegal** y que no se iba a repetir. Pero en ningún momento se le informa al paciente sobre su solicitud de accedo al documento firmado en la Tablet.

La AEPD trasladó la reclamación al hospital para que aportase las pruebas pertinentes para defenderse. Manifestaron que las empleadas de admisión, ante la gran afluencia de pacientes y en el contexto de pandemia, para que se cumpliesen las medidas de seguridad y con el fin de evitar el contagio, decidieron de forma puntual premarcar la casilla de los pacientes **"algo que nunca debió suceder".** Asimismo, destacaron que, tras la firma del documento, la paciente no solicitó en admisión una copia de la cláusula informativa a pacientes firmada, "pues de haberlo hecho, se le hubiera entregado".

Por otro lado, el hospital apuntó que una vez **tuvo conocimiento de lo sucedido** se implementaron medidas como, por ejemplo, formación del personal; se revisaron los procedimientos en relación con la formas de obtener el consentimiento de los interesados; se llevaron a cabo controles de forma aleatoria con varios consentimientos para ver si estaban marcadas o no todas las cláusulas; se modificó la base de legitimación para el tratamiento de los datos con la finalidad de envío de comunicaciones comerciales.

PROTECCIÓN DE DATOS CONSIDERA QUE SE HAN VULNERADO DOS ARTÍCULOS DEL RGPD

Consideraron que han tenido una actitud proactiva centrada en eliminar cualquier riesgo que pueda producirse en el tratamiento de los datos de los interesados.
Pero la AEPD ha determinado que el hecho de que el responsable del tratamiento de los datos personales obtenidos de los pacientes de la Clínica obtenga su consentimiento a través de un formulario donde las casillas de los fines a los que se destinaran los mismos, aparte de la gestión de la historia clínica del paciente, se encuentran ya marcadas en "acepto" vulnera el artículo 6.1 Y 15 del Reglamento General de Protección de Datos (RGPD).

Y aunque hayan reconocido el error y hayan tomado medidas, "esta actuación no produce en sí misma una reducción de los prejuicios sufridos por el paciente si no que lo único que se ha producido es la actuación obligada por la norma y para el futuro". Por tanto, le sancionó con 20.000 euros por ambas infracciones. Pero el 31 de octubre de 2022 efectuó el pago de **16.000 euros** haciendo uso de la reducción prevista en la propuesta de resolución.

BOLETÍN LOPD EN LA EMPRESA

AÑO 2022

edor team ANDALUCÍA
Software y Servicios para Asesorías y Empresas

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España,** es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 01/22

EL RGPD UE 2016/679 EN APLICACIÓN

El principio de minimización y las relaciones laborales

Uno de los principios que debemos tener en cuenta cuando tratamos datos personales es la minimización de los datos (art 5.c RGPD). **Este principio nos obliga como responsables del tratamiento que los datos personales sean adecuados, pertinentes y limitados a lo necesario para los fines objeto del tratamiento.**

Los datos personales necesarios para el desarrollo de la relación laboral, podrían ser los siguientes, y a título solamente ejemplificativo, (según la guía de la AEPD): el nombre y apellidos de la persona trabajadora; sexo; número de DNI; número de afiliación de extranjero y de la Seguridad Social; nacionalidad; discapacidad y fecha de nacimiento.

Otros datos personales que no resultan imprescindibles para la ejecución de un contrato, se podrían tratar por el empleador con una base jurídica diferente a la del contrato, como podría ser el interés legítimo. Para ello, habría que analizar las características de cada relación laboral. Así, por ejemplo, la dirección de correo electrónico o el número de teléfono personal, son datos que permiten a la empresa localizar a su personal y contactar con ellos en caso necesario. El tratamiento será preciso ponderarlo caso por caso.

Contenido

1. El principio de minimización y las relaciones laborales.
2. Sanción de 50.000€ a una constructora por una cesión ilícita de datos de salud de un trabajador.
3. Plan de Inspección de Oficio de la Atención Sociosanitaria (I) Historia sociosanitaria y documentación.
4. Cifrado y Privacidad (V): la clave como dato personal.
5. Cómo proteger la seguridad de la información en la empresa.

IMPORTANTE

El interés legítimo se tiene que demostrar debidamente aplicando los principios de ponderación y proporcionalidad.

SANCIONES DE LA AEPD

Sanción de 50.000€ a una constructora por una cesión ilícita de datos de salud de un trabajador

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00324-2021.pdf, una empresa constructora es sancionada por ceder datos de salud (bajas médicas, motivos y permisos) a otra empresa, así como la dirección del correo personal, sin el consentimiento del trabajador (reclamante).

La entidad sancionada manifiesta que envió la documentación referida, por requerimiento de la Entidad Pública Empresarial de Vivienda, para defenderse de las denuncias interpuestas por el reclamante por falta de adscripción de medios humanos y materiales en la obra en la que se encontraba trabajando.

En este sentido, la AEPD considera que se ha vulnerado el art 5.1.c del RGPD "Principio de minimización de datos". Se están tratando datos de salud (bajas y permisos por COVID) y datos de carácter personal (correo electrónico personal del trabajador) para una finalidad distinta a la de servir como medio de comunicación entre empresa y trabajador. **Los datos que la entidad reclamada ha aportado como alegaciones para su defensa se consideran excesivos.**

En calidad de agravantes, se estima el tratamiento de los datos de salud, como categorías especiales de datos. La multa que se le ha impuesto ascendió a la cantidad de 50.000€.

Principio de minimización de datos: los datos han de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines de su tratamiento

IMPORTANTE

El responsable debe realizar un tratamiento de datos de categorías especiales conforme a las excepciones dispuestas en el RGPD.

LA AEPD ACLARA

Plan de Inspección de Oficio de la Atención Sociosanitaria (I) Historia sociosanitaria y documentación

En el apartado de la AEPD Guías y Herramientas, encontramos el documento denominado "Plan de Inspección de Oficio de la Atención Sociosanitaria"

En este boletín y los siguientes analizaremos las recomendaciones más relevantes detalladas en este documento. **La AEPD analizó diferentes centros públicos y privados que prestan servicios sociosanitarios con atención directa a usuarios, siendo de ámbito estatal, regional y local y de diferentes tamaños. A lo largo del documento se recomiendan acciones de mejora.**

En el apartado de "Historia sociosanitaria y documentación", tras analizar la situación del tratamiento de los historiales sociosanitarios por parte de los centros auditados, se recomiendan las siguientes acciones:

-evitar la dispersión de documentos por diferentes departamentos, copias duplicadas, etc.: supone un riesgo en la integridad de la documentación al no poder realizar una actualización de la información adecuada.

- **digitalización total de la historia sociosanitaria del centro**: lo que permite acceder a ellas según las necesidades de los diferentes profesionales.

- **incluir registro de acceso**: cuando la digitalización no fuera posible, se instaurará un procedimiento de gestión de la documentación en papel, que incluya un registro de los accesos, para conocer en todo momento la trazabilidad de los datos personales.

IMPORTANTE
Crear procedimientos seguros para el traslado de la documentación sociosanitaria y aplicar una política de mesas limpias para evitar un acceso no autorizado de terceras personas.

ACTUALIDAD LOPD

Cifrado y Privacidad (V): la clave como dato personal

Fuente: AEPD

A la hora de aplicar criptografía, el uso de una clave es el parámetro determinante. Hay muchas definiciones de qué es una clave. Brevemente, podemos decir que una clave es un parámetro que determina el resultado de un algoritmo criptográfico. Atendiendo a la clave, los sistemas de cifrado se pueden dividir en dos grandes grupos: los cifrados simétricos, donde una única clave cifra y descifra; y los cifrados asimétricos, en los que se precisan de dos claves, una para cifrar, que puede tener carácter público, y otra, para descifrar, que tiene carácter privado y está únicamente en posesión de su legítimo titular. Las dos claves del cifrado asimétrico están vinculadas, pero es muy difícil deducir una de la otra si no se dispone de información adicional.

Los cifrados asimétricos están diseñados para que una de las claves se desvele y sea de libre acceso, la clave pública, por lo que son muy adecuados para su empleo en Internet. De esta forma, el uso de las claves asimétricas no solo permite el cifrado/descifrado de información, sino también realizar la autenticación de personas, la generación o la verificación de firmas, el intercambio de claves simétricas, etc.

Las claves públicas pueden ser empleadas por personas, entidades e incluso máquinas para identificarse, autenticarse o intercambiar información. Cuando se trata de claves públicas que corresponden a personas físicas cabría plantearse si estas claves se pueden considerar datos de carácter personal. A este respecto, tanto la autoridad francesa CNIL (Solutions for a responsible use of the blockchain in the context of personal data) como el Parlamento Europeo (Blockchain and the General Data Protection Regulation) ya han manifestado que son datos personales en el marco de tratamientos específicos.

Para determinar la naturaleza de datos de carácter personal de la clave pública hay que tener en consideración la propia definición de dato personal establecida en el artículo 4:

«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará 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, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona

Puede ver más información en el siguiente enlace

Innovación y Tecnología

EL PROFESIONAL RESPONDE

Cómo proteger la seguridad de la información en la empresa

En este apartado "El profesional responde", iremos abordando la importancia de conocer y desarrollar procedimientos para mantener la seguridad de la información de nuestra empresa.

Lo primero que tenemos que definir es el concepto de seguridad de la información. Todas las empresas independientemente de su tamaño tienen que proteger su información para poder seguir creciendo y cumpliendo sus objetivos profesionales. Así, por ejemplo, debemos aplicar medidas para garantizar la confidencialidad de los datos bancarios de nuestros clientes o la propiedad intelectual de nuestra empresa o las tarifas y ofertas que nos posicionan en el mercado.

Estos son algunos de los principales errores que se cometen en el tratamiento de la información y que ponen en peligro la seguridad de la información:

-carpetas de red compartidas sin control de acceso.

-Usuarios que aún conservan acceso a información que ya no es necesaria en su nueva posición en la empresa.

-Eliminar los ordenadores y discos sin analizar su contenido y eliminar la información confidencial.

-No realizar copias de seguridad de la información y asegurarnos que tenemos una copia de seguridad actualizada.

IMPORTANTE

Las empresas independientemente de su tamaño deben evitar riesgos en su activo vital más importante: la información.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 02/22

EL RGPD UE 2016/679 EN APLICACIÓN

Deber de secreto y seguridad en el ámbito laboral(I)

Contenido

1. Deber de secreto y seguridad en el ámbito laboral(I).
2. Sanción de 4.000€ a un taller mecánico por el envío de emails comerciales sin copia oculta.
3. Plan de Inspección de Oficio de la Atención Sociosanitaria (II) confidencialidad y obligaciones del personal.
4. Cómo gestionar tus derechos ante la recepción de publicidad no deseada.
5. Los pilares de la seguridad de la información: confidencialidad, disponibilidad e integridad.

En nuestra LOPDGDD, el deber de secreto y confidencialidad está recogido en el artículo 5" Deber de confidencialidad". En él se detalla que los responsables y encargados del tratamiento y todas las personas que intervengan en cualquier fase del tratamiento están sujetas al deber de confidencialidad**. Es decir, todo el personal laboral de la empresa debe estar informado de este deber de confidencialidad. El responsable, además, en virtud de la proactividad tendrá que demostrarlo.**

La obligación general de confidencialidad será complementaria de los deberes de secreto profesional. Además, este articulo señala que las obligaciones de confidencialidad y de secreto profesional se mantendrán, aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Por su parte, el responsable y encargado del tratamiento deben garantizar, no solamente, la confidencialidad, sino también, la disponibilidad de los datos, su pronta recuperación ante cualquier ataque y la integridad de los datos para que no puedan ser maliciosamente manipulados.

La empresa tiene que disponer de políticas de cumplimiento de estos dos principios.

IMPORTANTE

La vulneración del deber de confidencial es considerada una infracción grave en la LOPDGDD.

SANCIONES DE LA AEPD

Sanción de 4.000€ a un taller mecánico por el envío de emails comerciales sin copia oculta

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00259-2021.pdf, se sanciona a un taller mecánico por el envío de emails con carácter comercial, sin tener el consentimiento y, además, sin copia oculta.

El reclamante en su escrito de reclamación manifiesta que había recibido un correo comercial sin autorización previa. Además, estaban expuestos los datos de los demás destinatarios, incluyendo nombre y apellidos completos y dirección de correo electrónico. El reclamante en su escrito añadía, que no incluían ninguna opción para darse de baja. Como anexo a la reclamación, se adjuntan los datos completos del email recibido, con más de 400 destinatarios sin ocultar sus datos personales.

Se han incumplido varios preceptos del RGPD, por un lado, el principio de integridad y confidencialidad, unido a la falta de medidas de seguridad por parte del responsable para garantizar la confidencialidad de los datos personales. Como agravantes de la sanción se han tenido en cuenta el número de interesados afectados y la negligencia respecto a la gestión de la seguridad de los datos personales.

En este caso, además, el reclamante manifiesta que no dio su consentimiento para el envío de dichos correos comerciales, por lo que también la entidad es sancionada.

Principio de confidencialidad: tratar los datos que garanticen una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito.

IMPORTANTE

Para el envío de correos comerciales es necesario solicitar el consentimiento previo o bien existir una relación contractual previa.

LA AEPD ACLARA

Plan de Inspección de Oficio de la Atención Sociosanitaria (II) confidencialidad y obligaciones del personal

En el apartado de la AEPD Guías y Herramientas, encontramos el documento denominado "Plan de Inspección de Oficio de la Atención Sociosanitaria"

La confidencialidad en las operaciones de tratamiento en los centros sociosanitarios es un deber fundamental. **En estos centros se tiene un acceso generalizado a datos de categorías especiales. El cumplimiento del deber de confidencialidad debe llevarse al extremo.**

Aunque la mayoría de los colectivos profesionales que trabajan en los centros sociosanitarios están sujetos al secreto profesional, se debe complementar mediante un compromiso de confidencialidad escrito. **Este debe ser firmado por todos los empleados, becarios, estudiantes en prácticas, personal de empresas externas y en general, por cualquier persona con acceso a datos personales de los usuarios del centro. Los trabajadores sin acceso a datos personales, también deberían firmar un documento similar.**

Este documento debería contener:

-Prohibición general expresa de difundir, comunicar o revelar datos a terceras personas.

-Carácter indefinido del compromiso, inclusive extinguida la relación del trabajo con el centro.

-Información sobre las consecuencias y responsabilidades derivadas del incumplimiento.

IMPORTANTE

Se recomienda impartir formación e información sobre las obligaciones de protección de datos personales y entregar un acuse de recibo del documento informativo.

ACTUALIDAD LOPD

Cómo gestionar tus derechos ante la recepción de publicidad no deseada

Fuente: AEPD

A pesar de actuar de manera responsable a la hora de dar mis datos, no dar consentimiento para que los traten con finalidades publicitarias, inscribirme en la Lista Robinson y de haber seguido todos los consejos para prevenir la publicidad no deseada que presentábamos en esta entrega anterior de nuestro blog, es posible que sigas recibiendo algún tipo de comunicación comercial no deseada a través de llamadas de teléfono, mails, sms o mensajes a través de aplicaciones de mensajería instantánea.

A continuación, te presentamos una serie de consejos o acciones que puedes realizar para limitar la publicidad no deseada:

Utiliza las fórmulas que te ofrecen

Las comunicaciones electrónicas publicitarias ofrecen sistemas para que puedas rechazar el uso de tus datos con fines publicitarios, que incluyen medios como el envío de un correo electrónico a la dirección electrónica indicada, un SMS, un enlace o la opción de llamar a un número telefónico gratuito. Esta suele ser la manera más sencilla de dejar de recibir las comunicaciones comerciales de esa empresa, entidad u organización. Utilízala antes de pasar al resto de acciones que te presentamos.

Retira tu consentimiento

Si diste tu consentimiento cuando contrataste o te inscribiste en un servicio para que tratasen tus datos con fines publicitarios, puedes revocarlo en cualquier momento utilizando el método que la empresa ponga a tu disposición. Si desconoces o no encuentras la manera de hacerlo, puedes consultar el apartado dedicado a la protección de datos de su página web.

Ejerce tu derecho de oposición

Puedes ejercer este derecho ante la entidad responsable del tratamiento para solicitar que te excluya de las campañas publicitarias que realice. Si lo haces, indica claramente en la solicitud que no deseas que traten tus datos con fines publicitarios e informa del canal por el que estás recibiendo la publicidad y los datos que no deseas que se traten. Por ejemplo, si recibes publicidad telefónica, puedes indicar tu número de teléfono para que no lo utilicen con fines comerciales.

En el espacio dedicado a los derechos de nuestra web dispones de más información sobre el mismo y formularios tipo para ejercerlo ante el responsable. (…)

Puede ver más información en el siguiente enlace

Publicidad no deseada

EL PROFESIONAL RESPONDE

Los pilares de la Seguridad de la Información: confidencialidad, disponibilidad e integridad

Cuando escuchamos el término de Seguridad de la Información, casi de forma inmediata, se nos viene a la cabeza el término de confidencialidad de la información. Este es uno de los pilares en los que se sustenta la Seguridad de la información, pero no el único. La disponibilidad de la información y la integridad son dos aspectos de la información que también deben mantenerse a salvo.

La confidencialidad se refiere a que la información solo sea accesible al personal, entidades o sistemas autorizados para su acceso. Como ejemplo de esta falta de confidencialidad sería la divulgación no autorizada a través de las redes sociales de información confidencial, o el acceso por parte de un empleado a la información crítica de la empresa sin permiso asignado.

La disponibilidad de la información se refiere a que esta siempre esté accesible cuando la vayamos a utilizar. Como ejemplo de esta falta de disponibilidad, cuando existe un ataque de denegación de servicio y no podemos acceder a la información.

Y, por último, la integridad de la información supone que la información sea correcta y no sufra modificaciones no controlados o errores. Como ejemplo, podría ser la alteración de forma fraudulenta de los ficheros del sistema informático mediante la explotación de una vulnerabilidad.

IMPORTANTE

Se deben evaluar estas tres dimensiones de la información en los activos de información que emplea la empresa para implantar las medidas adecuadas.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 03/22

EL RGPD UE 2016/679 EN APLICACIÓN

Deber de secreto y seguridad en el ámbito laboral (II)

Contenido

1. Deber de secreto y seguridad en el ámbito laboral (II).
2. Una empresa de educación es sancionada con 9.000 euros por publicar imágenes de su personal laboral en RRSS.
3. Plan de Inspección de Oficio de la Atención Sociosanitaria (III) Información ofrecida al usuario.
4. La AEPD publica una lista de verificación para ayudar a los responsables a realizar evaluaciones de impacto.
5. Garantizar la seguridad de la información con la implementación de medidas.

Dos de los principios fundamentales en el tratamiento de los datos en el ámbito laboral son el deber de secreto y seguridad. El responsable en el ejercicio de sus actividades debe garantizar el secreto y la seguridad en el tratamiento de los datos personales, y, además, debe demostrarlo. Por ello, se hace necesario que se apliquen medidas técnicas y organizativas imprescindibles.

Algunas de estas medidas podrían ser las enumeradas a continuación:

- Diseñar funciones y responsabilidades de la plantilla de personal.
- Formar adecuadamente a las personas trabajadoras según el grado de responsabilidad que contribuya a crear una cultura de compromiso con la protección de datos.
- Advertir y formar, inclusive, los perfiles que no tienen relación directa con el tratamiento de datos personales.
- Valorar la designación de un delegado de protección de datos, con expertos formados en la materia, que asesoren en el cumplimiento de la normativa y el principio de responsabilidad proactiva.

El incumplimiento del deber de secreto y seguridad suponen graves perjuicios para la empresa y su reputación.

IMPORTANTE

La falta de adopción de medidas técnicas y organizativas para aplicar los principios de protección de datos supone una sanción grave.

SANCIONES DE LA AEPD

Una empresa de educación es sancionada con 9.000 euros por publicar imágenes de su personal laboral en RRSS

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00119-2021.pdf, se sanciona a una empresa dedicada a prestar servicios de educación por la publicación de imágenes de su personal laboral en las redes sociales y en la página web corporativa.

El reclamante, en su escrito, aporta copia de los correos que envió a la dirección web del reclamado para que retirara sus fotos de la página web y redes sociales. También envía un archivo con fotografías web bajo el rótulo de "Equipo educativo".

La AEPD inicia el procedimiento sancionador ya que la empresa a incumplido lo dispuesto en el RGPD.

Por un lado, la reclamada no tenía legitimación para el tratamiento de los datos personales del afectado, puesto que, para la publicación de imágenes del personal laboral en la página web de la empresa y RRSS se requiere el consentimiento expreso de los trabajadores/as. **La relación laboral no legitima al responsable para la publicación de imágenes.**

Además, el responsable no respondió al derecho de supresión solicitado por el reclamante, hasta en dos ocasiones, tal y como consta en el escrito de reclamación.

La multa ascendió a un total de **9.000 euros.**

El responsable debe aplicar medidas de seguridad que garanticen la confidencialidad de los datos.

IMPORTANTE

La publicación de imágenes se considera una cesión a terceros por lo que debe ser debidamente informada y legitimada por el responsable de los datos.

LA AEPD ACLARA

Plan de Inspección de Oficio de la Atención Sociosanitaria (III) Información ofrecida al usuario

En el apartado de la AEPD Guías y Herramientas, encontramos el documento denominado "Plan de Inspección de Oficio de la Atención Sociosanitaria"

En este plan de inspección de Oficio, la AEPD analiza la información que se le ofrece al usuario en materia de protección de datos. **Las conclusiones a la que ha llegado, entre otras, es que en la mayoría de los centros auditados carecen de carteles informativos en las zonas de recepción o en otras zonas de acceso de los pacientes. Además, se ha detectado que existían carteles desactualizados con referencia a la normativa antigua.** En los formularios adaptados al RGPD se evidencia cierta confusión cuando se informa de la base jurídica o licitud.

La AEPD da una serie de recomendaciones para solventar las deficiencias analizadas:

- Colocación de carteles informativos sencillos, actualizados y de fácil lectura para los usuarios, en las zonas de acceso al centro.
- Informar siempre en el momento de la recogida de los datos y no en el momento del ingreso u otro posterior.
- La segunda capa de información debe ser consultada por el usuario inmediatamente de forma sencilla ya sea a su solicitud o por consulta on-line.
- Facilitar una copia al usuario cuando se utilice un solo documento informativo que sea firmado por el usuario para dejar acreditada la información facilitada.

IMPORTANTE

La información facilitada al usuario debe ser accesible a los usuarios, utilizando un lenguaje claro y sencillo.

ACTUALIDAD LOPD

La AEPD publica una lista de verificación para ayudar a los responsables a realizar evaluaciones de impacto

Fuente: AEPD

(Madrid, 17 de febrero de 2022). La Agencia Española de Protección de Datos (AEPD) ha publicado una lista de verificación para ayudar a los responsables del tratamiento a identificar y determinar de una forma rápida si el proceso y la documentación que están siguiendo para llevar a cabo una Evaluación de Impacto en la Protección de Datos (EIPD) contiene **los elementos exigibles**.

La AEPD cuenta con la guía 'Gestión del riesgo y evaluación de impacto en tratamientos de datos personales', que facilita la obligatoria gestión de riesgos en los procesos de gobernanza de las entidades y, cuando corresponda, la EIPD. **Este listado de verificación complementa esa guía** y permite, una vez desarrollada y documentada la Evaluación de Impacto, **efectuar una comprobación final** para cerciorarse de que se han tenido en cuenta todos los aspectos recogidos en la normativa de protección de datos.

El Reglamento General de Protección de Datos establece que las organizaciones que tratan datos personales deben realizar una gestión del riesgo con el fin de **establecer medidas para garantizar los derechos y libertades de las personas**. Además, en aquellos casos en los que los tratamientos impliquen un riesgo alto para la protección de datos, el Reglamento dispone que esas organizaciones están obligadas a realizar una Evaluación de Impacto en Protección de Datos para mitigar esos riesgos. Si tras la realización de la EIPD, y después de haber adoptado medidas, el riesgo sigue siendo alto, el responsable debe llevar a cabo una consulta previa a la autoridad de control antes de realizar ese tratamiento de datos personales.

El objetivo de este nuevo recurso de la AEPD es ayudar a los responsables a cumplir con las obligaciones de desarrollar y documentar una EIPD y para que, en caso de tener que realizar esa consulta previa a la Agencia, sea más sencillo comprobar que se cumple con los requisitos para su presentación, en particular los que se derivan de la Instrucción 1/2021, por la que se establecen directrices respecto de la función consultiva de la Agencia.

En este sentido, en caso de que los responsables del tratamiento tengan previsto realizar una consulta previa, la Instrucción 1/2021 establece que estos deberán contemplar lo señalado por la AEPD en sus guías y recomendaciones. En consecuencia, **el responsable deberá presentar esta lista de verificación cumplimentada** ante la Agencia, con el fin de incluir el contenido mínimo exigido y dotar a su consulta de mayor precisión y exactitud.

Puede ver más información en el siguiente enlace

Gestión del riesgo y evaluación de impacto en tratamientos de datos personales

EL PROFESIONAL RESPONDE

Garantizar la seguridad de la información con la implementación de medidas

Recientemente, el Tribunal Supremo ha dictado una sentencia relevante para la seguridad de los datos personales.

En este sentido, el Tribunal Supremo manifiesta que la obligación del responsable por mantener la seguridad de los datos es una obligación de medios y no de resultados. Es decir, a la hora de exigir responsabilidades, no puede hacerse sobre el hecho ya producido, sino sobre la diligencia de la implementación de las medidas.

Como responsables de la seguridad de la información tenemos que aplicar las medidas de seguridad en nuestra entidad teniendo en cuenta dos fases:

A) Análisis de la adecuación de medidas: En esta fase verificaremos que las medidas se ajustan al análisis de riesgos previo, que en la selección de medidas se han tenido en cuenta la probabilidad y el impacto de los riesgos identificados y en esta primera fase, además, comprobaremos que las medidas se han implantado de forma completa.

B) Análisis de la efectiva aplicación de las medidas: en esta segunda fase verificamos que las medidas se han implantado de forma completa, que están activas y siguen siendo las idóneas y que con su implantación evitan razonablemente las brechas de seguridad que puedan producirse.

IMPORTANTE

No basta con diseñar medios técnicos y organizativos necesarios, se hace imprescindible su correcta implementación y utilización.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 04/22

EL RGPD UE 2016/679 EN APLICACIÓN

La importancia del registro de las actividades de tratamiento (I)

En primer lugar, acudimos a la definición que el RGPD hace de tratamiento como: ***"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no."***

Estas operaciones pueden ser, por ejemplo, la recogida de datos en un formulario de inscripción, la conservación de los datos en formato digital o papel para la finalidad por la cual se recogieron.

Todos los responsables y encargados de tratamiento tienen que realizar un registro de las actividades de tratamiento que efectúan bajo su responsabilidad. Este registro contendrá, entre otros:

- Nombre y datos de contacto del responsable y, en su caso, del corresponsable, representante y delegado de protección de datos.
- Fines del tratamiento.
- Categoría de interesados y datos personales.
- Categoría de destinatarios.
- Transferencias internacionales y sus garantías.
- Plazos previstos para la supresión de datos.
- Descripción general de las medidas de seguridad.

Contenido

1. La importancia del registro de las actividades del tratamiento (I).
2. Sancionado un Hotel con 30.000€ por utilizar la fotografía del pasaporte para el control de pagos.
3. Guía para la notificación de brechas de datos personales a la autoridad de control (I).
4. Las reclamaciones presentadas ante la AEPD aumentaron un 35% en 2021.
5. Garantizar la seguridad de la información: seguridad en redes wifi (I).

IMPORTANTE

La LOPDGDD considera infracción grave no disponer del registro de actividades de tratamiento conforme a la normativa.

SANCIONES DE LA AEPD

Sancionado un Hotel con 30.000€ por utilizar la fotografía del pasaporte para el control de pagos

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00078-2021.pdf se sanciona a un hotel por utilizar la fotografía del pasaporte de los clientes para controlar los pagos que realiza el huésped durante su estancia.

El reclamante, un ciudadano holandés, interpuso la reclamación ante la Autoridad de control de Países Bajos, y se dio traslado a la AEPD, que actuó como autoridad de control principal. Aunque en un principio la autoridad española no encontró indicios de incumplimiento, la autoridad belga formuló objeciones al procedimiento, por lo que finalmente, la entidad reclamada fue sancionada.

El Hotel, en cumplimiento de la obligación de registro documental, tal y como se recoge en la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, tomaba los datos del huésped en el *check-in*. Además de los datos, escaneaban una copia del pasaporte que incluía la fotografía.

La autoridad de control sancionó al hotel por el uso posterior que se hace de esa fotografía. El hotel alegó que la fotografía servía de medio para evitar que se realizaran pagos fraudulentos con la tarjeta de crédito del cliente. A ella solo podía acceder el personal autorizado.

La autoridad de control entendió que el interés legítimo alegado para ese tratamiento no era el adecuado.

Los datos utilizados deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

IMPORTANTE

El responsable debe realizar un juicio de ponderación cuando alegue el interés legítimo para el tratamiento de datos personales.

LA AEPD ACLARA

Guía para la notificación de brechas de datos personales a la autoridad de control (I)

En el apartado de la AEPD Guías y Herramientas, encontramos el documento denominado Guía para la notificación de brechas de datos personales.

En esta guía se dan las indicaciones necesarias al responsable del tratamiento para notificar, en su caso, a la autoridad de control competente, las brechas de seguridad.

Si el incidente de seguridad, no afecta a datos personales o a tratamientos de datos personales, no se trataría de una brecha de datos. Tampoco se consideran brechas, cuando el tratamiento se lleve a cabo por personas físicas en el ámbito doméstico.

No es obligatorio notificar todas las brechas. El RGPD prevé una excepción cuando el responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo.

Por otro lado, en la guía se hace referencia a que si lo que se pretende es denunciar por la posible vulneración de la normativa de un empleado, o tercero, el canal utilizado es el de presentación de reclamaciones.

El responsable del tratamiento es quién debe notificar a la autoridad de control. Aunque, este puede autorizar a una persona física, o representante. El encargado de tratamiento que ha sido objeto de la brecha, también podrá notificar a la autoridad de control siempre y cuando así venga establecido en el contrato.

En la sede electrónica encontramos el formulario en línea que permite hacer las notificaciones telemáticas.

IMPORTANTE

En todo tratamiento hay que determinar el riesgo que para los derechos y libertades puede suponer que se materialice una brecha de datos personales.

ACTUALIDAD LOPD

Las reclamaciones presentadas ante la AEPD aumentaron un 35% en 2021

Fuente: AEPD

(21 de marzo de 2022). La Agencia Española de Protección de Datos (AEPD) ha publicado hoy su Memoria 2021, que recoge de forma exhaustiva las actividades realizadas, las cifras de gestión, los informes y procedimientos más relevantes del año, y un análisis de los retos presentes y futuros. La actividad de organismo en 2021 ha estado centrada de forma prioritaria en una doble vertiente: **dar respuesta a los desafíos de protección de datos relacionados con la pandemia y seguir impulsando que aquellos que tratan datos** se comprometan con la protección de la privacidad. En el primer bloque, la Agencia ha continuado participando en articular garantías para proteger los datos personales en los tratamientos relacionados con las medidas contra la COVID-19, tanto en un plano nacional como en el europeo a través del Comité Europeo de Protección de Datos (CEPD). En el segundo, en 2021 se puso en marcha el Pacto Digital para la Protección de las Personas, una iniciativa que ya cuenta con casi 400 entidades adheridas y que promueve la privacidad y la ética digital como un activo que las organizaciones deben tener en cuenta a la hora de diseñar sus políticas y sus estrategias.
En cuanto a las cifras de gestión, en 2021 se han presentado ante la Agencia **13.905 reclamaciones, un aumento de un 35% respecto a 2020. Esta cifra asciende a las 14.571** incluyendo los casos transfronterizos, los casos en los que la Agencia actúa por iniciativa propia y las quiebras de seguridad trasladadas a inspección. En 2021 las **reclamaciones resueltas han aumentado un 35% (14.098**) respecto al año anterior (10.443), una cifra muy destacable que ha permitido resolver reclamaciones pendientes de ejercicios anteriores sin que hayan aumentado significativamente los tiempos medios de resolución. En esos tiempos de tramitación de las reclamaciones hay que hacer una referencia a los **traslados**, una previsión recogida por la LOPDGDD para facilitar la resolución rápida de las reclamaciones y que ha permitido que estas se resuelvan en menos de dos meses. (…)

En cuanto a las reclamaciones ordinarias, las **planteadas con mayor frecuencia** por los ciudadanos en 2021 corresponden a servicios de internet (16%), videovigilancia (12%), recepción de publicidad (excepto spam) (11%) e inserción indebida en ficheros de morosidad (9%). En cuanto a los procedimientos sancionadores, se finalizaron 585, un 49% más que en 2021. Las áreas más frecuentes en los procedimientos sancionadores son videovigilancia (25%), servicios de internet (22%), y publicidad a través de correo electrónico o teléfono móvil (9%).

Se han realizado 264 resoluciones que han finalizado con la imposición de multa. Las seis **áreas de actividad con mayor importe global de multas** han sido la publicidad (8.659.200 euros), telecomunicaciones (6.500.000 euros), entidades financieras/ acreedoras (6.243.000 euros), ficheros de morosidad (4.209.000 euros), contratación fraudulenta (3.674.000 euros) y asuntos laborales (2.625.900 euros).

Puede ver más información en el siguiente enlace

Memoria 2021

EL PROFESIONAL RESPONDE

Garantizar la seguridad de la información: seguridad en redes wifi (I)

Existen muchos tipos de redes inalámbricas, dependiendo de la arquitectura, tecnología o estándares de comunicación. En este blog nos referiremos a las Redes de Área Local inalámbricas (WLAN).

Los componentes de la red wifi son los denominados dispositivos cliente, que solicitan la conexión a la red inalámbrica. Pueden ser, por ejemplo, las *tablets*, los ordenadores portátiles, etc. **Y los puntos de acceso, (conocido como *router*)** que sirven como puertas de enlace a otras y conecta los dispositivos clientes entre ellos.

Dependiendo de la forma en que se intercambien los datos en la red, esta puede ser de dos tipos:

- Mod Ad Hoc, en este caso, no existen puntos de acceso. Los dispositivos se comunican entre sí, por ejemplo, a través de tecnologías como bluetooth.
- Mod infraestructura, es la que utilizamos normalmente en las casas y empresas. El punto de acceso (*router*) es el que nos conecta con otros dispositivos, impresoras, servidores, etc.

La utilización de este tipo de redes inalámbricas nos permite tener una gran movilidad y, a varios usuarios conectándose a la vez desde cualquier lugar donde llegue la señal. Además, no habrá que preocuparse del mantenimiento del cableado.

IMPORTANTE

La utilización de este tipo de redes conlleva la realización de un pormenorizado análisis de riesgos para mitigar los riesgos inherentes a estas redes wifi.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 05/22

EL RGPD UE 2016/679 EN APLICACIÓN

Listado de tratamientos concretos de la LOPDGDD (II)

Contenido

1. Listado de tratamientos concretos de la LOPDGDD (II).
2. Multinacional sancionada con 250.000€ por un protocolo inadecuado de atención de derechos.
3. Guía para la notificación de brechas de datos personales a los afectados (II).
4. Brechas de datos personales: entornos de desarrollo y preproducción.
5. Los principales riesgos y amenazas en las redes inalámbricas (II).

En el anterior boletín nos referíamos a la importancia del registro de actividades de tratamiento. **En nuestra ley orgánica (LOPDGDD) se regulan una serie de tratamientos de forma concreta. El responsable del tratamiento debe tenerlo en cuenta para aplicar la normativa adecuadamente.**

Los tratamientos regulados son los siguientes:

- Tratamiento de datos de contacto, empresarios individuales y de profesionales liberales.
- Tratamiento de los sistemas de información crediticia.
- Tratamientos relacionados con operaciones mercantiles.
- Tratamiento con fines de videovigilancia.
- Sistemas de exclusión publicitaria.
- Sistemas de información de denuncias internas.
- Tratamiento de datos en el ámbito de la función estadística pública.
- Tratamiento de datos con fines de archivo en interés público.
- Tratamiento de datos relativos a infracciones y sanciones administrativas.

Añadiríamos en este listado, aquellos que vengan indicados en su normativa específica.

IMPORTANTE

Todos los responsables y encargados de tratamiento tienen que realizar un registro de las actividades de tratamiento que efectúan bajo su responsabilidad.

SANCIONES DE LA AEPD

Multinacional sancionada con 250.000€ por un protocolo inadecuado de atención de derechos

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00003-2021.pdf se sanciona a una multinacional, consultora líder a nivel internacional en selección de candidatos.

No contestar en el plazo de un mes una solicitud de derechos supone una infracción grave.

La reclamante, una ciudadana holandesa, interpuso la reclamación ante la Autoridad de control de Países Bajos, y se dio traslado a la AEPD, que actuó como autoridad de control principal, al encontrarse el servicio de cumplimiento legal de la multinacional en Barcelona. Aunque en un principio, la autoridad española no encontró indicios de incumplimiento, varias autoridades europeas formularon objeciones al procedimiento, por lo que finalmente, la entidad reclamada fue sancionada.

La reclamante manifestó que envió su CV a la citada multinacional a través de su página web mediante contraseña y usuario. Solicitando un tiempo después el ejercicio del derecho de acceso a sus datos personales. Para ello, se le requirió por parte de la entidad reclamada, que debía aportar su DNI.

En la resolución la AEPD, estimó que solicitar el DNI para identificar al interesado del ejercicio del derecho resultaba excesivo, ya que, existían otros medios de comprobación, como el usuario y contraseña de la reclamada. No se tuvo en cuenta el principio de minimización de datos. Se le sancionó con 250.000€.

IMPORTANTE

La entidad reclamada no había implementado un protocolo adecuado para atender el ejercicio de derechos en materia de protección de datos.

LA AEPD ACLARA

Guía para la notificación de brechas de datos personales a los afectados (II)

En el apartado de la AEPD Guías y Herramientas, encontramos la Guía para la notificación de brechas de datos personales.

En esta guía se concretan los supuestos en los que el responsable del tratamiento tiene que notificar la brecha de datos personales a los interesados afectados. Estos son todas las personas físicas cuyos datos personales se han visto afectados por una brecha y les puede ocasionar consecuencias.

El responsable deberá comunicar a la mayor brevedad posible cuando exista un alto riesgo para los derechos y libertades de las personas, la falta de confidencialidad, integridad o disponibilidad de sus datos. Incluyendo, la falta de disponibilidad de los servicios asociados a esos datos personales. Se comunicará siempre que los daños producidos sean irreversibles.

En cambio, no será necesaria la comunicación cuando, el responsable haya tomado medidas técnicas y organizativas adecuadas, que eviten los riesgos, que minimicen los daños, o bien, que los haga reversibles. Tampoco será necesaria su comunicación, cuando con posterioridad a la brecha, el responsable haya adoptado medidas que mitiguen total o parcialmente el posible impacto. **Así, por ejemplo, cuando aplique medidas como la revocación, cancelación o bloqueo de credenciales de acceso o el restablecimiento del servicio y copias de seguridad que faciliten la disponibilidad e integridad de los datos.**

Tanto la decisión de comunicar, o la no necesidad de comunicar debe ser documentada.

IMPORTANTE

La AEPD ha publicado el informe de brechas de seguridad del mes de marzo de 2022

ACTUALIDAD LOPD

Brechas de datos personales: entornos de desarrollo y preproducción

Fuente: AEPD

La ingeniería de sistemas establece la conveniencia de trabajar con varios entornos diferenciados: habitualmente, desarrollo, preproducción y producción. De forma general, lo recomendable es trabajar en el entorno de desarrollo, realizar las pruebas en el entorno de preproducción y finalmente desplegar aplicaciones y servicios en el entorno de producción. Desde la óptica de protección de datos, hay que tener en cuenta esta diferenciación y limitar la exposición de datos personales reales, y/o que estén en los sistemas de producción, en las fases de desarrollo y pruebas por el riesgo que puede suponer para los derechos y libertades de las personas.

Todavía es habitual encontrar entornos de desarrollo y preproducción en los que las medidas técnicas y organizativas orientadas a implementar las medidas y garantías establecidas en el Reglamento General de Protección de Datos (RGPD) se relajan, o quedan expuestos a internet sin medidas de seguridad o abandonados y en desuso por lo que las medidas de seguridad pronto quedan obsoletas. Pero tampoco hay que olvidar que en algunos casos se empleen datos reales para pruebas de depuración de errores en labores de mantenimiento y/o desarrollo.

Con la aplicación del RGPD y la LOPDGDD, la situación respecto al uso de datos personales para pruebas en general, y en particular en entornos de desarrollo, se puede resumir brevemente a continuación.

En primer lugar, el RGPD en su artículo 32 Seguridad del tratamiento, establece que el responsable y el encargado de tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de los interesados. Luego el responsable y el encargado deben determinar las medidas de seguridad apropiadas con respecto al uso de datos personales reales en entornos de preproducción y pruebas. Además, deben establecer estas medidas teniendo en cuenta el nivel de riesgo específicamente con relación a la protección de datos, de igual forma que han de tener en cuenta los riesgos para la organización, como en cualquier entorno de producción. (…)

Conforme al principio de minimización de datos y el principio de protección de datos desde el diseño y por defecto, cuando sea posible debe evitarse la utilización de datos personales en entornos de desarrollo y preproducción, o cualquier otro entorno de pruebas.

Además, las pruebas de software con datos personales son, o forman parte de, tratamientos de datos personales y el responsable del tratamiento debe cumplir con todas las obligaciones que se desprenden del RGPD.

Puede ver más información en el siguiente enlace

Innovación y Tecnología

EL PROFESIONAL RESPONDE

Los principales riesgos y amenazas en las redes inalámbricas (II)

Se hace necesario, hoy en día, conocer las principales amenazas a las que se encuentran expuestas las redes inalámbricas. Su conocimiento nos podrá ser de utilidad para aplicar medidas de seguridad adecuadas.

Ataques por fuerza bruta: Con este método se pretende hacer uso de todas las contraseñas posibles y averiguar las claves criptográficas de aquellas que dan acceso a la red wifi. En Internet se pueden encontrar herramientas gratuitas para hacerse con aquellas claves de redes que no tengan claves robustas.

Denegación de servicio: A través de este ataque envían peticiones de servicio masivas a los puntos de acceso sobrecargándoles, de manera que se impide a los usuarios legítimos hacer uso del servicio que presta.

Man-in-the-middle: El atacante se sitúa entre el emisor y el receptor, suplantando a una de las partes. De esta forma se hace creer a la otra parte que está hablando con el legítimo destinatario de la comunicación.

Mac Spoofing: Con este tipo de ataques se trata de suplantar la dirección *MAC,* que es un identificador único e irrepetible que identifica todo dispositivo conectado a una red. Este ataque se produciría siempre y cuando el punto de acceso tuviera configurada una lista de este tipo de direcciones permitidas.

IMPORTANTE

Realizar un análisis de riesgos adecuado a la entidad, podría reducir las consecuencias de las amenazas de las redes inalámbricas.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 06/22

EL RGPD UE 2016/679 EN APLICACIÓN

Tratamientos concretos: Sistema de denuncias internas

En nuestra Ley orgánica LOPDGDD se regula el tratamiento concreto del sistema de denuncias internas. **Este sistema permite poner en conocimiento de una entidad, incluso de forma anónima, la comisión de actos o conductas que puedan resultar contrarias a la normativa general o sectorial, ocurridos en la propia entidad, o bien, en la actuación con terceros que contraten con ella.**

En el art. 24 de la LOPDGDD se regulan aspectos concretos del sistema de denuncias interna. Señalamos a continuación alguno de ellos:

- La licitud del tratamiento proviene de la existencia de un interés público.
- Los empleados y terceros deben ser informados de la existencia del sistema.
- El acceso se limita a los que tienen funciones de control interno y cumplimiento.
- Deben adoptarse medidas necesarias para preservar la identidad y confidencialidad.
- Los datos se conservarán durante el tiempo necesario para decidir si se inicia una investigación. A los tres meses se suprimirán.
- Transcurrido el plazo anterior, los datos se tratarán por el órgano correspondiente, para la investigación de los hechos.

Contenido

1. Tratamientos concretos: Sistema de denuncias internas.
2. Multan a un restaurante por publicar el nombre y apellidos de una extrabajadora en las reseñas de Google.
3. El nombramiento y funciones del delegado de protección de datos.
4. La AEPD sanciona a Google LLC por ceder datos a terceros sin legitimación y obstaculizar el derecho de supresión.
5. Seguridad en el correo electrónico corporativo: Política de seguridad (I).

IMPORTANTE

El Ministerio de Justicia ha aprobado el anteproyecto de Ley que regulará la creación de los sistemas y los derechos y garantías del informante.

SANCIONES DE LA AEPD

Multan a un restaurante por publicar el nombre y apellidos de una extrabajadora en las reseñas de Google

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00395-2021.pdf se sanciona a un restaurante por la publicación de los datos personales de una extrabajadora en las reseñas de Google.

La reclamante denunció ante la AEPD la publicación de sus datos personales en Internet. Manifiesta que el propietario del restaurante en el que trabajaba respondió a las reseñas negativas que habían publicado en Google, alegando que las criticas venían de parte de los amigos de la reclamante, y para ello, identificó a la extrabajadora con nombre y apellidos, revelando, además, las circunstancias de su sanción laboral.

Junto a la reclamación, aporta cuatro capturas de pantalla, con el título *"Respuesta del propietario",* en las que se visualiza la contestación a diferentes reseñas, en las cuáles, incluye el nombre y apellidos de la reclamante.

La Subdirección General de Inspección procedió a la realización de actuaciones previas de investigación, solicitando información a la entidad reclamada, sin obtener respuesta alguna por parte de esta. **Finalmente, la AEPD, a la vista de los hechos, le impuso una sanción de 1.500 €** por la infracción del art.5.1. f, falta de confidencialidad y el art.6.1.a el tratamiento es ilícito por la publicación sin el consentimiento.

Son sanciones consideradas muy graves, la vulneración del deber de confidencialidad.

IMPORTANTE

La publicación de datos de terceros en Internet requiere del consentimiento del interesado afectado, salvo que, esté exceptuado legalmente.

LA AEPD ACLARA

El nombramiento y funciones del Delegado de Protección de Datos

El Gabinete jurídico de la AEPD publicó un informe sobre las funciones y nombramiento del delegado de protección de datos.

La AEPD ha ido señalando de forma reiterada el papel fundamental que dentro del modelo de responsabilidad activa desempeña el delegado de protección de datos. Su nombramiento no se debe interpretar solamente como una formalidad, sino que, se tendrán que aplicar todos los requisitos que se recogen en la normativa aplicable.

Uno de estos requisitos, es la asignación de funciones, que como mínimo serán las recogidas en la norma, entre las que se encuentran, las funciones de asesoramiento y supervisión dirigidas a garantizar un adecuado cumplimiento de la normativa de protección de datos. **Por su parte, tanto el responsable como el encargado del tratamiento, establecerán los medios necesarios para que el delegado de protección de datos pueda participar de forma adecuada y en tiempo oportuno de las cuestiones relativas a la protección de datos personales.**

En cuanto a los requisitos de capacitación, el RGPD dispone que el delegado de protección de datos será designado atendiendo a sus cualidades profesionales, y en particular, a los conocimientos especializados que tenga del Derecho y la práctica en materia de protección de datos, así como su capacidad para desempeñar las funciones que la normativa de protección de datos le asigne.

IMPORTANTE

La cualificación del delegado de protección de datos podrá demostrarse a través de mecanismos de certificación.

ACTUALIDAD LOPD

La AEPD sanciona a Google LLC por ceder datos a terceros sin legitimación y obstaculizar el derecho de supresión

Fuente: AEPD

(18 de mayo de 2022). La Agencia Española de Protección de Datos (AEPD) ha dictado resolución del procedimiento iniciado contra la compañía Google LLC en la que declara la existencia de **dos infracciones muy graves** de la normativa de protección de datos e impone una sanción de **10 millones de euros** por ceder datos a terceros sin legitimación para ello y obstaculizar el derecho de supresión de los ciudadanos (artículos 6 y 17 del Reglamento General de Protección de Datos).

Google LLC es la responsable del tratamiento analizado y lo lleva a cabo en EEUU. En el caso de la **comunicación de datos a terceros**, la Agencia ha constatado que Google LLC envía al Proyecto Lumen información de solicitudes que le realizan los ciudadanos, incluida su identificación, dirección de correo electrónico, los motivos alegados y la URL reclamada. La misión de ese proyecto es la recogida y puesta a disposición de solicitudes de retirada de contenido, por lo que la Agencia considera que, dado que se remite toda la información contenida en la solicitud del ciudadano para que se incluya en otra base de datos accesible al público y para que se divulgue a través de una web, "supone en la práctica frustrar la finalidad del ejercicio del derecho de supresión".

La resolución recoge que esta comunicación de datos por parte de Google LLC al Proyecto Lumen se impone al usuario que pretenda utilizar sus formularios, **sin opción de oponerse** a la misma y, por tanto, sin que exista un consentimiento válido para que esa comunicación se lleve a cabo. Establecer esta condición en el ejercicio de un derecho reconocido a los interesados no está amparado por el Reglamento General de Protección de Datos al generarse "un tratamiento adicional de los datos sobre los que versa la solicitud de supresión al comunicarlos a un tercero". Además, en la política de privacidad de Google LLC, no se hace mención a este tratamiento de datos personales de los usuarios, y tampoco aparece entre las finalidades la comunicación al Proyecto Lumen.

La AEPD también recoge en su resolución que, presentada la solicitud de retirada de contenido y atendido el derecho, es decir, acordada la supresión de los datos personales, "no cabe un tratamiento posterior de los mismos, como es la comunicación que Google LLC realiza al Proyecto Lumen".

En cuanto al ejercicio de derechos de los ciudadanos, la AEPD detalla en su resolución que "es difícil deducir si la solicitud se formula invocando la normativa de protección de datos personales, sencillamente porque esta normativa no se menciona en ninguno de los formularios, con independencia del motivo que el interesado seleccione de entre las opciones propuestas, salvo en el formulario denominado 'Retirada en virtud de la ley de privacidad de la UE', el único disponible que contiene una referencia expresa a esta normativa".

Puede ver más información en el siguiente enlace

Expediente N.º: PS/00140/2020

EL PROFESIONAL RESPONDE

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

El correo electrónico es una herramienta de comunicación corporativa que facilita y agiliza el funcionamiento en una empresa. **A pesar de sus grandes beneficios como la accesibilidad, rapidez y la posibilidad de adjuntar archivos, se hace necesario definir un uso correcto y seguro.** En algunas ocasiones, los empleados/as pueden enviar documentos confidenciales a quien no debían por error, o bien desvelar la dirección de correo electrónico de clientes o usuarios. **En este sentido es muy importante concienciar al personal, a los usuarios/as del correo corporativo de las amenazas y dotarles de las herramientas adecuadas para que hagan un uso seguro del correo.**

La entidad debería elaborar unas Políticas de seguridad, en concreto, para el uso del correo electrónico. **Estas Políticas como mínimo tendrían que contener:**

- Normativa de uso de correo electrónico.
- Instalar aplicaciones antimalware y antispam.
- Instalar tecnología de cifrado y firma digital.
- Desactivar el formato HTML, ejecución de macros y descarga de imágenes.
- Contraseña segura. Elaboradas conforme a la Política de contraseñas.
- Identificación de correos sospechosos.
- Normas para evitar el uso de las redes públicas.

IMPORTANTE

Una utilización segura del correo electrónico corporativo evitaría caer en las trampas de los ciberdelincuentes.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 07/22

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

1. Tratamientos concretos: Sistemas exclusión publicitaria.
2. Un laboratorio es sancionado con 20.000€ por comunicar los resultados del test COVID-19 de una trabajadora.
3. Los servicios de vigilancia de la salud son responsables de informar al trabajador/a de la comunicación de sus datos.
4. Metaverso y privacidad.
5. Seguridad en el correo electrónico corporativo: Política de seguridad (II).

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.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 08/22

EL RGPD UE 2016/679 EN APLICACIÓN

Tratamientos concretos: Sistemas de Información crediticia

En nuestra LOPDGDD, en concreto, el articulo 20 regula estos sistemas de información crediticia conocidos como ficheros de morosos.

El tratamiento de los datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito, será lícito, siempre y cuando se cumplan los siguientes requisitos:

- Los datos tienen que ser facilitados por el acreedor o por quién actúe por su cuenta o interés.
- Los datos se refieren a deudas ciertas, vencidas y exigibles. Además, no tiene que existir reclamación administrativa o judicial por parte del deudor.
- El acreedor debe informar al afectado en el contrato, o bien en el momento de requerir el pago, de la posibilidad de inclusión en un fichero de morosos.

La entidad que mantenga los ficheros, relativos al incumplimiento de las deudas, definidas con anterioridad, debe notificar al afectado la inclusión de sus datos. Le informará, también, sobre la posibilidad del ejercicio de los derechos en materia de protección de datos. El plazo para informar será de 30 días desde la notificación de la deuda. Durante ese plazo los datos deben quedar bloqueados.

Contenido

1. Tratamientos concretos: Sistemas de información crediticia.
2. Sancionado al propietario de tres páginas online por no informar debidamente a los internautas.
3. Consejos de la AEPD para proteger nuestros datos en vacaciones.
4. La AEPD publica una guía dirigida a los profesionales del sector sanitario
5. La seguridad en la nube: conceptos básicos(I).

IMPORTANTE

Los datos podrán ser consultados por aquellos que mantengan una relación contractual con el afectado y los que vayan a celebrar contratos de crédito al consumo y crédito inmobiliario.

SANCIONES DE LA AEPD

Sancionado al propietario de tres páginas online por no informar debidamente a los internautas

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00542-2021.pdf se sanciona al propietario de tres páginas web por informar indebidamente a los usuarios y no recoger el consentimiento para el tratamiento de los datos personales.

La reclamación fue interpuesta por una sociedad jurídica que reclamaba ante la AEPD la inexistencia de información en las tres páginas web del reclamado. En los formularios de contacto no había ninguna referencia sobre la propiedad de las webs.

La AEPD en su fase de investigación, constató el funcionamiento de los formularios. A través del enlace "contacto", la web redirige al usuario a una nueva página donde se pueden introducir datos personales como el nombre o el correo electrónico. Una vez introducidos los datos personales en el formulario, no existe casilla de aceptación de la política de privacidad. Se pueden enviar los datos personales directamente haciendo click en "enviar". **En el apartado de los formularios tampoco existe ningún enlace que redirija al usuario a la "Política de Privacidad".**

El titular de las tres páginas web fue sancionado con 2.000€ por no recoger el consentimiento mediante una casilla de aceptación y, además, por no informar debidamente. **En la "Política de Privacidad" no aparecía ningún dato relacionado con la identidad del responsable del tratamiento.**

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

IMPORTANTE

El responsable debe cumplir con el principio de Transparencia e información. Facilitará al interesado toda la información básica del tratamiento de sus datos y le indicará el modo de acceder al resto información.

LA AEPD ACLARA

Consejos de la AEPD para proteger nuestros datos en vacaciones

En la página web de la AEPD en su apartado de guías, herramientas e infografías, encontramos una infografía con consejos para proteger nuestros datos personales en esta época estival.

Durante las vacaciones de verano, no se puede bajar la guardia y hay que seguir siendo activos en la protección de datos. En esta infografía, la AEPD nos da algunos consejos de cómo afrontar situaciones de riesgo.

1. Piensa dos veces antes de compartir una foto o vídeo: Los códigos de billetes y tarjetas de embarque contienen datos personales y del viaje.
2. Evita decir dónde estás: Compartir en internet fotografías de viajes o geolocalización a través de una aplicación puede facilitar información a los delincuentes.
3. Desconfía de las Wifis abiertas o públicas: Las redes abiertas pueden ser utilizadas por ciberdelincuentes para robarte datos personales y contraseñas. No intercambies información sensible ni te conectes a tu servicio de banca.
4. Adelántate al robo o pérdida de tus dispositivos: La AEPD nos recomienda que hagamos una copia de seguridad de la información que almacenamos, así como, añadir un sistema de clave o patrón para bloquear los dispositivos.

IMPORTANTE

Si tuvieras que conectarte desde un ordenador público de un hotel o un locutorio, utiliza la navegación privada del navegador y no guardes contraseñas en el dispositivo compartido.

ACTUALIDAD LOPD

La AEPD publica una guía dirigida a los profesionales del sector sanitario

Fuente: AEPD

(Madrid, 22 de junio de 2022). La Agencia Española de Protección de Datos (AEPD) ha publicado la 'Guía para profesionales del sector sanitario', un documento que **responde a las dudas más frecuentes que pueden surgir a los profesionales que intervienen en la prestación de servicios sanitarios** y que tiene por objeto facilitar el cumplimiento de la normativa de protección de datos y la garantía de los derechos de los usuarios de estos servicios.

La Guía está dirigida principalmente a los profesionales sanitarios **que desempeñen su actividad a título individual**, aunque sus orientaciones pueden resultar de utilidad para aquellos que trabajen **en el marco de establecimientos sanitarios**. Los datos de salud tienen la condición de categorías especiales y, por tanto, cuentan con un régimen reforzado de protección. En 2021 la AEPD registró 680 reclamaciones vinculadas a la sanidad, lo que representa un 75% más que en 2020, según datos de la última Memoria anual.

El documento aborda cuestiones que se plantean a menudo en este sector, como la legitimación para tratar datos de salud; quién puede acceder a la historia clínica y en qué casos; la responsabilidad y obligaciones derivadas de estos tratamientos, así como la gestión de los derechos de los pacientes o de las situaciones que puedan implicar comunicación de datos a terceros.

La Guía comienza analizando el **concepto de datos de salud**, así como la posición jurídica de quienes intervienen en la prestación de servicios sanitarios, como responsables del tratamiento o como prestadores de servicios a dichos responsables. Asimismo, se detallan las **bases jurídicas** para el tratamiento de los datos, diferenciando las específicas de los derechos de autonomía del paciente y las del tratamiento de datos personales, que incluyen otras bases de legitimación sin necesidad de consentimiento. En este apartado se abordan, entre otros interrogantes, si es necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes para tratar sus datos personales o podría ampararse en otras bases jurídicas; si pueden tratarse posteriormente los datos con finalidades distintas a la asistencia sanitaria o si puede constar el nombre y apellido de los profesionales en las tarjetas identificativas.

Por otro lado, el acceso a la historia clínica constituye un aspecto esencial de la asistencia sanitaria, por lo que la guía facilita **orientaciones** sobre quiénes pueden acceder a la misma para las distintas finalidades para las que están legitimados –profesionales sanitarios, residentes, centros sociosanitarios o centros privados concertados– así como los riesgos y responsabilidades en que pueden incurrir quienes accedan ilícitamente.

Puede ver más información en el siguiente enlace

Guía para profesionales del sector sanitario

EL PROFESIONAL RESPONDE

La seguridad en la nube: conceptos básicos(I)

Hoy en día, el término de *cloud computing* está presente en nuestro ámbito profesional. Se trata de una nueva forma de prestación de los servicios de tratamiento de la información. Podemos contratar diferentes servicios en la nube, como, por ejemplo, servidores de ficheros, *backup*, alojamiento, web, CRM y ERP, videoconferencias, etc. La nube nos permite utilizar recursos que facilitan la conexión desde cualquier lugar, la unificación de recursos y una implementación rápida.

En este entorno, la gestión de la información está de forma virtual en manos del cliente que contrata los servicios de la nube. El proveedor del servicio puede encontrarse, en cualquier lugar del mundo, y proporcionar los servicios *cloud* a través de, por ejemplo, prácticas de deslocalización, movilidad o realizando subcontrataciones adicionales. **Así, en este caso, el contratista puede desconocer la localización concreta de sus datos y, por lo tanto, no disponer del control directo de acceso y portabilidad. Todo esto nos lleva a tener que ser rigurosos en el momento de la contratación de un servicio de este tipo.** Para elegir aquel proveedor que cumpla con toda la legislación, y en especial, con la normativa en protección de datos y seguridad, son muchos los aspectos a tener en cuenta en este nuevo entorno *cloud*, que iremos analizando en los siguientes boletines.

IMPORTANTE

La empresa que utilice la nube como recurso debe tener una política de clasificación de información que indique que tipo puede subir al *cloud.*

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 09/22

EL RGPD UE 2016/679 EN APLICACIÓN

Roles en la protección de datos: el responsable de tratamiento

Contenido

1. Roles en la protección de datos: el responsable de tratamiento.
2. Una Comunidad de Propietarios es sancionada con 6.000€ por incumplir la normativa de protección de datos.
3. Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo (I).
4. Empleo de datos biométricos: evaluación desde la perspectiva de protección de datos.
5. La seguridad en la nube: amenazas y riesgos (II).

En los siguientes boletines vamos a ir tratando los diferentes roles que operan en el tratamiento de los datos personales. **En la normativa en protección de datos, se regulan tres figuras que son; el responsable del tratamiento, el encargado del tratamiento y el corresponsable.** A estas tres, además, tenemos que sumar una figura fundamental, a resultas del carácter proactivo de la norma, este es el delegado de protección de datos.

Es importante diferenciar cada una de ellas. En el artículo 4 del RGPD, se define al responsable, como *"aquella persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medio del tratamiento"*. **Es decir, el responsable, es el que decide sobre determinados aspectos esenciales del tratamiento de los datos.** Preguntarnos acerca de por qué tiene lugar el tratamiento y quién ha decidido que debe llevarse a cabo el tratamiento para ese fin concreto, ayuda a definir el rol del responsable.

El responsable siempre decide sobre los fines del tratamiento. En cambio, respecto de los medios, podemos diferenciar entre medios esenciales y no esenciales. En los no esenciales puede decidir el encargado del tratamiento.

IMPORTANTE

Para ser considerado responsable no es necesario disponer de un acceso real a los datos que esté tratando.

SANCIONES DE LA AEPD

Una Comunidad de Propietarios es sancionada con 6.000€ por incumplir la normativa de protección de datos

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00523-2021.pdf, se sanciona con 6.000€ a una Comunidad de propietarios por el incumplimiento de varios preceptos de la normativa de protección de datos.

La reclamación es interpuesta por una propietaria de la comunidad. En su escrito manifestó, que, durante el verano del 2020, para entrar en la piscina comunitaria, le exigían que mostrara su DNI, el cuál era apuntado por el vigilante contratado, en un papel en blanco, a la vista del resto de usuarios de la piscina. La reclamante se puso en contacto con el presidente de la comunidad, el cual, le comunicó que se recogía ese dato por la situación de pandemia COVID-19 para facilitarlo al Ministerio de Sanidad en caso de brote. Esa decisión fue tomada solamente, en Junta directiva, pero no vecinal, tal y como manifestó la administradora de fincas.

La AEPD, en su fase de investigación, envío escrito de notificación a la Comunidad de propietarios para que enviara alegaciones, pero no presentó nada al respecto. **Se sanciona a la Comunidad con 6.000€ por excederse en el tratamiento de los datos, ya que, con apuntar el piso y letra hubiera sido suficiente para identificar al usuario de la piscina.** Además, también, se le sanciona por no informar debidamente del tratamiento de los datos personales.

La falta de información a los interesados/as en el tratamiento de sus datos supone una falta muy grave en nuestro ordenamiento jurídico.

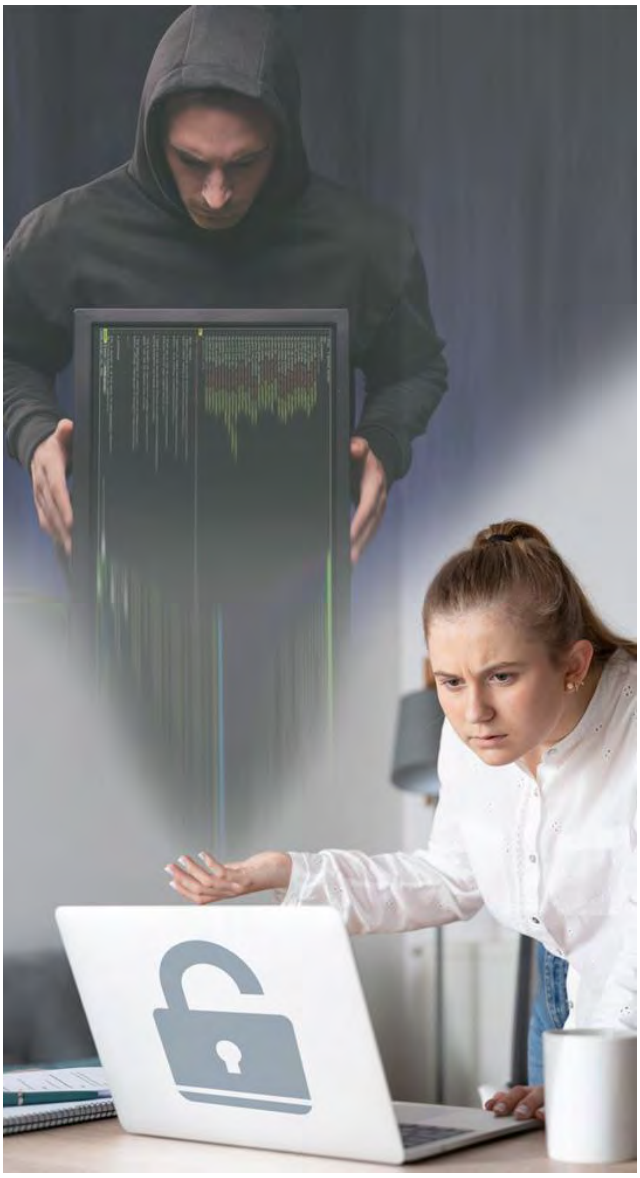
IMPORTANTE

Los datos personales tienen que ser los adecuados, pertinentes y limitados a lo necesario en relación con los fines del tratamiento.

LA AEPD ACLARA

Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo (I)

La Unidad de Evaluación y Estudios Tecnológicos de la AEPD, editó unas recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo. Estas recomendaciones están dirigidas a responsables del tratamiento y al personal que participa en las operaciones de tratamiento.



Las recomendaciones para el responsable son:

1º Definir una política de protección de la información para situaciones de movilidad. Entre otros aspectos, se determinarán que formas de acceso remoto se permiten, qué tipo de dispositivos son válidos para cada forma de acceso y el nivel de acceso permitido en función de los perfiles. Se informará al usuario de las amenazas en que pueden verse afectados al trabajar fuera de la organización.

2º Elegir soluciones y prestadores de servicio confiables y con garantías. Cuando accedan a datos de carácter personal, tendrán la consideración de encargados de tratamiento que se regirá por un contrato de acceso a datos.

3º Restringir el acceso a la información. Dependiendo de los perfiles o niveles de acceso a los recursos y a la información.

4º Configurar periódicamente los equipos y dispositivos utilizados en situaciones de movilidad.

5º Monitorizar los accesos realizados a la red corporativa desde el exterior.

IMPORTANTE

En la política de protección de la información para situaciones de movilidad se informará sobre el alcance de las actividades de control y supervisión.

ACTUALIDAD LOPD

Empleo de datos biométricos: evaluación desde la perspectiva de protección de datos

Fuente: AEPD

Los tratamientos que incluyen operaciones con datos biométricos se pueden emplear con muchas finalidades: prueba de vida, identificación, autenticación, seguimiento, perfilado, decisiones automáticas, etc. Las operaciones biométricas pueden emplear distintas técnicas, algunas de forma simultánea, y, a su vez, una misma técnica se puede implementar de formas diferentes. Las operaciones con datos biométricos en un tratamiento concreto tendrán un grado distinto de intrusión e impacto en la privacidad de los individuos que dependerá de la técnica empleada, pero también de la propia definición del tratamiento, su naturaleza, el ámbito o alcance en el que se va a desarrollar, su contexto y, en especial, los fines que se persiguen. Por lo tanto, la evaluación de impacto de las operaciones biométricas se ha de realizar en el marco de un tratamiento y con relación a sus fines últimos.

Las técnicas de proceso de datos biométricos se basan en recoger y procesar rasgos físicos, conductuales, fisiológicos o neuronales de las personas mediante dispositivos o sensores, creando firmas o patrones que posibilitan la identificación, seguimiento o perfilado de las personas. Algunos métodos requieren la cooperación de la persona, mientras que otros métodos pueden capturar datos biométricos a distancia, sin requerir la cooperación del individuo y sin que pueda tener conciencia de ello.

En el marco de un tratamiento, cualquiera de las distintas técnicas biométricas que se incluyan tienen que ser evaluadas de acuerdo con la adecuación, proporcionalidad y la necesidad, su finalidad, su el impacto en los derechos y libertades de las personas físicas y los riesgos que conllevan, tanto para el individuo como para la sociedad.

Existen distintos criterios de clasificación de los sistemas biométricos: algunos basados en el uso de tecnologías diferentes, otros relacionados con los dispositivos o sensores, otros con relación al rasgo o conjuntos de rasgos estudiados, etc. Sin embargo, a la hora de demostrar la adecuación de un tratamiento al Reglamento General de Protección de Datos (RGPD), y de evaluar el riesgo para los derechos y libertades de los individuos que puede suponer el procesamiento de dichos datos, es conveniente emplear criterios de clasificación de las operaciones biométricas desde el punto de vista de protección de datos y con relación al tratamiento en el que se implementa.

La validación de las técnicas biométricas empleadas en un tratamiento ha de realizarse “desde el diseño” tal y como exige el artículo 25.1 del RGPD y con las recomendaciones que establece en la Guía de Privacidad desde el Diseño. El análisis de estos factores, y otros que puedan ser específicos del tratamiento o de la operación biométrica elegida, permitirán realizar un análisis del cumplimiento normativo, de la necesidad y proporcionalidad del tratamiento permitiendo una gestión del riesgo más adecuada.

Puede ver más información en el siguiente enlace

Nota técnica: 14 equívocos con relación a la identificación y autenticación biométrica

EL PROFESIONAL RESPONDE

La seguridad en la nube: amenazas y riegos (II)

La gestión de las amenazas y riesgos que conlleva la utilización de los servicios *cloud,* resulta imprescindible para mantener el control sobre la información y garantizar su protección y disponibilidad en cualquier momento. Vamos a enumerar las principales amenazas, riesgos y su mitigación.

Entre las amenazas podemos destacar las amenazas internas de empleados/as insatisfechos o exempleados/as que pueden provocar situaciones de riesgo cuando no se gestionan los permisos y privilegios de acceso. El problema del uso de las tecnologías compartidas puede provocar que por un fallo de seguridad usuarios de otras empresas accedan a nuestra información. La suplantación de identidad, es otra de las amenazas, cuando los ciberdelincuentes por ingeniería social se hacen con las credenciales de algún usuario.

Un análisis de riesgos adecuado a la empresa, nos garantiza una gestión del riesgo que permita mitigarlo. Por ejemplo, ante el riesgo de falta de aislamiento de los datos, para gestionar su mitigación, los datos en reposo deben estar aislados y los procedimientos de cifrado ejecutados por personal formado. La empresa debe saber dónde está localizada la información más sensible y adoptar medidas de protección. Otro ejemplo, para evitar la indisponibilidad del servicio, hay que exigir a los proveedores una óptima capacidad de recuperación de datos y el tiempo estimado.

IMPORTANTE

Para reducir los riesgos en la nube se tiene que aplicar el mismo concepto de seguridad que se exige en las instalaciones físicas.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 10/22

EL RGPD UE 2016/679 EN APLICACIÓN

Roles en la protección de datos: el encargado de tratamiento

Contenido

1. Roles en la protección de datos: el encargado de tratamiento.
2. La Subdirección General de Inspección de Datos sanciona con 80.000€ a una empresa corredora de seguros
3. Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo (II).
4. La Agencia y el Supervisor Europeo lanzan un documento que identifica los 10 errores más comunes sobre "*machine learning* y protección de datos"
5. La seguridad en el comercio electrónico. Tipos de comercio electrónico (I)

El encargado de tratamiento es otro de los roles imprescindibles a tener en cuenta en materia de protección de datos. Su definición la encontramos en el artículo 4.8 del RGPD: "***persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".***

En la normativa de protección de datos existen varios artículos que regulan y determinan las funciones del encargado del tratamiento. **En concreto, nuestra LOPDGDD, en el artículo 33, indica que, cuando el encargado utilice para su propia finalidad los datos facilitados por el responsable por cuenta de quién actúa, tendrá la consideración de responsable**. Esto significa que se le podrán aplicar las mismas cuantiosas sanciones que al responsable del tratamiento.

El contrato de acceso a datos, es el nombre que le damos al contrato celebrado entre el responsable del tratamiento y el encargado. **Su contenido íntegro se encuentra regulado en el artículo 28.3 del RGPD.** En él se deben indicar, entre otros aspectos, la duración, la naturaleza, la finalidad del tratamiento, el tipo de datos personales y categorías de interesados y las obligaciones y derechos del responsable. La falta de este contrato supone una falta grave.

IMPORTANTE

El encargado del tratamiento seguirá las instrucciones del responsable incluidas aquellas referidas a las transferencias internacionales.

SANCIONES DE LA AEPD

La Subdirección General de Inspección de Datos sanciona con 80.000€ a una empresa corredora de seguros

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00401-2022.pdf, la Subdirección General de Inspección de datos (SGID), inspeccionó de oficio a la entidad sancionada puesto que tenía conocimiento de actuaciones que podrían vulnerar la legislación en materia de protección de datos.

Varias entidades, responsables y encargados del tratamiento del sector seguros notificaron, a la División de Innovación Tecnológica de la AEPD, la publicación no autorizada de datos de sus clientes. La entidad sancionada, hizo público en distintos foros la venta de usuarios de una compañía de seguros dedicada al sector del automóvil, además de los registros con información personal de clientes españoles de una compañía de seguros.

La AEPD, consideró que la corredora de seguros, como proveedora de servicios de gestión e infraestructuras tecnológicas, no contaba con las medidas organizativas técnicas y tecnológicas apropiadas para impedir la exposición de los datos personales de los asegurados.

Las infracciones cometidas se refieren a los artículos 5.1.f del RPGD "principio de integridad y confidencialidad" y al artículo 32 del RGPD "seguridad del tratamiento". La cantidad ascendió a 80.000€. Finalmente, la sanción se redujo a 48.000€ aplicando las reducciones.

La recepción de una reclamación de brecha de seguridad no implica una sanción directa, se debe analizar la diligencia de responsables y encargados de las medidas de seguridad aplicadas.

IMPORTANTE

El responsable y encargado de tratamiento deben realizar un análisis de riesgos para determinar las medidas técnicas y organizativas apropiadas.

LA AEPD ACLARA

Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo (II)

Las recomendaciones editadas por la Unidad de Evaluación y Estudios Tecnológicos de la AEPD, se dirigen también, además de al responsable del tratamiento, al personal que participa en las operaciones de tratamiento.

Estas recomendaciones deben estar recogidas en la política de teletrabajo.

1. Se debe respetar la política de protección de la información en situaciones de movilidad definida por el responsable.
2. **Proteger el dispositivo. Se tienen que definir y utilizar contraseñas de acceso robustas**. No se deben descargar ni instalar aplicaciones que no hayan sido autorizados. Si el equipo utilizado para establecer la conexión remota es personal, debe evitarse simultanear la actividad personal con la profesional y definir perfiles independientes para cada tipo de tarea.
3. Garantizar la protección de la información. Evitar exponer la pantalla a la mirada de terceros. **Si se trabaja habitualmente desde lugares públicos, es recomendable utilizar un filtro de privacidad para la pantalla.** Si se trabaja con papel, minimizar la entrada y salida de documentación en este soporte.
4. **Guardar la información en los espacios de red habilitados.** No se debe bloquear o deshabilitar la política de copia de seguridad.
5. **Comunicar de forma inmediata cualquier anomalía que afecte a la seguridad de la información.**

IMPORTANTE

Una vez concluida la jornada laboral en situación de movilidad debe desconectarse la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo.

ACTUALIDAD LOPD

La Agencia y el Supervisor Europeo lanzan un documento que identifica los 10 errores más comunes sobre "*machine learning* y protección de datos"

Fuente: AEPD

(Madrid, 20 de septiembre de 2022). La Agencia Española de Protección de Datos (AEPD) y el Supervisor Europeo de Protección de Datos (EDPS) han publicado un nuevo documento conjunto en el que exponen los 10 malentendidos más comunes relacionados con el *machine learning* (aprendizaje automático) y aportan un análisis de cuál debería ser el enfoque correcto.

El objetivo de estos documentos (versión en español y en inglés) es dilucidar los conceptos erróneos más comunes que rodean a los sistemas de *machine learning*, además de subrayar la importancia de implementar estas tecnologías de acuerdo con los valores de la UE, los principios de protección de datos y el respeto a los derechos de las personas.

La UE ha identificado la inteligencia artificial (IA) como una de las tecnologías más relevantes del siglo XXI, y ha destacado su importancia en la estrategia para la transformación digital de la UE. Al tener una amplia gama de aplicaciones, la IA puede contribuir en áreas tan dispares como el tratamiento de enfermedades crónicas, la lucha contra el cambio climático o la anticipación de amenazas de ciberseguridad.

"Inteligencia artificial", sin embargo, es un término general que engloba a aquellas tecnologías que tienen como objetivo imitar las capacidades de razonamiento humano, que pueden tener aplicaciones y limitaciones muy diferentes. Con frecuencia, los proveedores de tecnología promocionan sus sistemas haciendo referencia a la IA y, sin especificar qué tipo de IA.

El aprendizaje automático (*Machine Learning* o *ML*) es una rama específica de la IA, aplicada a la resolución de problemas específicos y limitados, como tareas de clasificación o predicción. A diferencia de otros tipos de IA que intentan emular la experiencia humana (por ejemplo, sistemas expertos); el comportamiento de los sistemas de aprendizaje automático no está definido por un conjunto predeterminado de instrucciones.

Los modelos de *ML* se entrenan utilizando conjuntos de datos. Durante su entrenamiento, los sistemas de *ML* se adaptan de forma autónoma a los patrones encontrados en las diferentes variables de un conjunto de datos dado, creando correlaciones. Una vez entrenado, el sistema utilizará los patrones aprendidos para generar un resultado.

El objetivo de este documento es dilucidar los conceptos erróneos comunes que rodean a los sistemas de *ML*, al tiempo que subrayar la importancia de implementar estas tecnologías de acuerdo con los valores de la UE, los principios de protección de datos y el total respeto a las personas.

Puede ver más información en el siguiente enlace

10 MALENTENDIDOS SOBRE EL *MACHINE LEARNING* (APRENDIZAJE AUTOMÁTICO)

EL PROFESIONAL RESPONDE

La seguridad en el comercio electrónico. Tipos de comercio electrónico (I)

La digitalización es un proceso que sigue en un imparable ascenso y aplica a todos los ámbitos de la vida. Con especial relevancia se han impuesto los medios electrónicos como medio de comunicación y consumo.

Hoy en día, son muchas las empresas que utilizan el comercio electrónico como principal método de negocio. Se conoce comúnmente como *e-commerce* en el cuál el pago lo realizamos mediante medios electrónicos.

En este boletín y siguientes vamos a definir los diferentes tipos de comercio electrónico en función de cómo se produce el intercambio entre el comprador y vendedor y las medidas de seguridad adecuadas para garantizar una venta segura.

- Tienda Online: realización de ventas a través de Internet.
- De afiliación: La venta, se realiza en una plataforma diferente a la tienda online. Esta plataforma se llevará una comisión de la venta.
- *Dropshipping*: el vendedor no envía el producto, lo hace un tercero.
- *Marketplace:* es una tienda que alberga a su vez varias tiendas.
- Membresía: compras recurrentes a través de suscripciones periódicas.
- Servicios: venta de servicios a través de Internet.

IMPORTANTE

Cada uno de los diferentes tipos de comercio electrónico deben garantizar una compraventa segura al consumidor.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 11/22

EL RGPD UE 2016/679 EN APLICACIÓN

Roles en la protección de datos: el corresponsable del tratamiento

Contenido

1. Roles en la protección de datos: el corresponsable del tratamiento.
2. Empresa sancionada con 70.000 € por infringir la normativa de protección de datos.
3. Privacidad y seguridad en Internet: ¿tengo obligación de dar mis datos cuando me los piden?
4. Guía y Herramienta básica de anonimización.
5. La seguridad en el comercio electrónico: medidas de ciberseguridad. Protocolos de seguridad.

En la normativa de protección de datos encontramos regulada la figura del corresponsable del tratamiento en el artículo 26 del RGPD. **En este caso, cuando nos encontramos ante la situación de que dos o más responsables determinan de forma conjunta los objetivos y los medios de tratamiento serán considerados corresponsables.**

Lo más importante de esta figura es que las decisiones sobre el tratamiento de datos personales se determinan de forma transparente y de mutuo acuerdo. En particular, deberán definir los siguientes aspectos:

- Ejercicio de los derechos del interesado
- Deber de informar al interesado

La figura de la corresponsabilidad no tiene que estar presente en todo el tratamiento de datos personales, sino solamente en aquellas etapas del tratamiento en el que sea necesario determinar los fines y los medios conjuntamente.

Todos los aspectos relativos a protección de datos, tendrán que reflejarse en un acuerdo y este acuerdo deberá ponerse a disposición del interesado.

IMPORTANTE

Los interesados podrán ejercer los derechos ante cualquiera de los responsables que figuren en el acuerdo de corresponsabilidad.

SANCIONES DE LA AEPD

Empresa de reparto sancionada con 70.000 € por infringir la normativa de protección de datos

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00280-2022.pdf, se sanciona a una conocida empresa de reparto por haber actuado en contra de los principios de la normativa de protección de datos.

La reclamante manifestó en su escrito que se habían cedido datos personales sin su consentimiento, puesto que el paquete que deberían haberle entregado a ella al encontrarse ausente, se lo entregaron a una vecina de su comunidad sin que ella hubiera manifestado su consentimiento.

Ante esta reclamación, la empresa de mensajería alega que en los términos de su contrato se recoge la posibilidad de entrega al vecino si el receptor no estuviera disponible salvo que se excluya esta opción. Ante lo cual, el establecimiento online donde fue comprado el producto debería haber marcado esta excepción.

La AEPD dispone en su resolución que no se puede hacer responsable al establecimiento ya que no existía ninguna relación de encargado del tratamiento y por lo tanto el comercio online no tenía instrucciones de cómo realizar el tratamiento. Se le sanciona con **50.000 €** por infringir el art.5.1. f del RGPD ante la falta de confidencialidad y con **20.000 €** por no haber aplicado medidas de seguridad adecuadas que garantizasen la confidencialidad en el tratamiento de los datos.

Se considera una infracción grave la falta de diligencia en la aplicación de medidas de seguridad técnica y organizativas que minimicen los riesgos del tratamiento de los datos personales.

IMPORTANTE

El responsable del tratamiento debe aplicar medidas de seguridad técnicas y organizativas adecuadas para garantizar la confidencialidad de los datos.

LA AEPD ACLARA

Privacidad y seguridad en Internet: ¿tengo obligación de dar mis datos cuando me lo piden?

La privacidad y la seguridad en Internet, hoy en día, es un aspecto fundamental que ha de estar presente en el tratamiento de los datos personales. La AEPD junto con otros organismos, INCIBE (Instituto Nacional de Ciberseguridad) y OSI (Oficina de Seguridad del Internauta) en su guía de Privacidad y seguridad en Internet, **dan consejos y recomendaciones prácticas para proteger los datos personales y no dar más información de la necesaria:**

1. Antes de facilitar los datos personales se debe analizar quién es el responsable que los está pidiendo y la finalidad.
2. **Cualquier información que te identifique o pueda permitir que alguien lo haga es un dato personal, como, por ejemplo, nombre y apellido, correo electrónico o la dirección *IP.***
3. No se debe facilitar información personal de terceros, salvo que te hayan dado su consentimiento, o bien seas el tutor o representante legal.
4. **Dar más información de la necesaria puede resultar perjudicial, tu privacidad e identidad se pueden ver comprometidas.**
5. Podemos ser víctima de extorsión o chantaje cuando facilitamos información que no es necesaria para la finalidad del tratamiento.

Existen excepciones en los que no se requiere el consentimiento para el tratamiento de datos personales, tales como, para proteger intereses vitales y cuando exista una ley que lo habilite.

IMPORTANTE

El responsable del tratamiento debe facilitar la información sobre el tratamiento de los datos personales, entre otros, la finalidad, la cesión y el plazo de conservación de los datos.

ACTUALIDAD LOPD

Guía y Herramienta básica de anonimización

Fuente: AEPD

(Madrid, 2 de noviembre de 2022). La Agencia Española de Protección de Datos (AEPD) ha publicado la 'Guía básica de anonimización', un documento elaborado por la Autoridad Nacional de Protección de Datos de Singapur (PDPC) y que, en colaboración con dicha autoridad, se ha traducido por su **valor didáctico y especial interés** para responsables, encargados de tratamientos y delegados de protección de datos.

Esta guía tiene como objetivo proporcionar una introducción y orientación práctica a las organizaciones sin experiencia previa en anonimización para que tengan orientaciones sobre **cómo realizar anonimización básica y desidentificación de conjuntos de datos**.

El documento dedica un capítulo específico a explicar la diferencia entre los **conceptos de anonimización** –conversión de datos personales en datos que no puedan utilizarse para identificar a ningún individuo–; **desidentificación**, que consiste en la eliminación de identificadores (nombre, dirección, número de documento nacional de identidad, etc.) que identifican directamente a un individuo, y **reidentificación**, referida a la identificación de individuos a partir de un conjunto de datos que previamente fue desidentificado o anonimizado.

Asimismo, aborda los **conceptos básicos de anonimización**, como el propósito y utilidad de esta técnica, reversibilidad, características, información inferida o las herramientas disponibles en el mercado. Posteriormente, desglosa el **proceso de anonimización** en cinco pasos: Conozca sus datos; Desidentifique sus datos; Aplique técnicas de anonimización; Calcule su riesgo y Gestione sus riesgos. La guía se complementa con una herramienta gratuita (descargable a través de este enlace) para que las organizaciones puedan transformar conjuntos de datos simples aplicando técnicas de anonimización.

Finalmente, el documento repasa las principales **técnicas de anonimización** de datos, los atributos comunes de los datos y las técnicas de anonimización sugeridas, la k-anonimidad, la evaluación del riesgo de reidentificación y las herramientas de anonimización.

Estos recursos están especialmente orientados a servir a pymes y startups cuando se tienen que enfrentar a la anonimización de pequeños conjuntos de datos, y también a aquellos que se quieren introducir en los principios de anonimización.

Puede ver más información en el siguiente enlace

Guía básica de anonimización

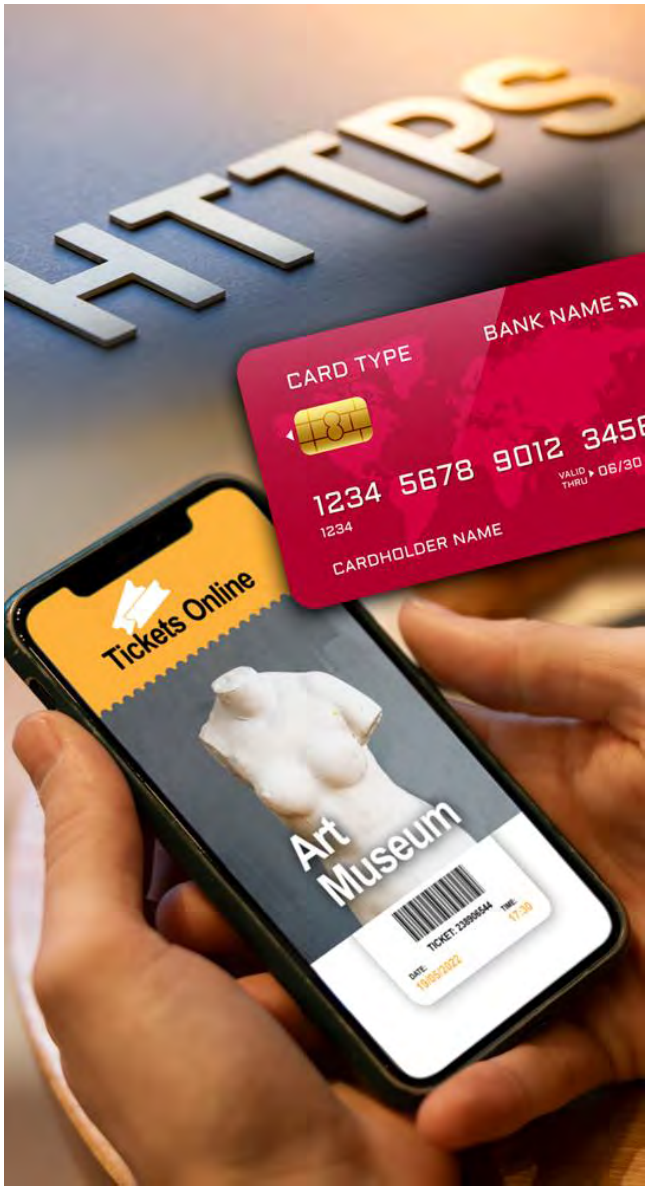
Herramienta básica de anonimización

EL PROFESIONAL RESPONDE

La seguridad en el comercio electrónico: medidas de ciberseguridad. Protocolos de seguridad

La aplicación de medidas de ciberseguridad garantiza a nuestros clientes una compra segura. **Los principales protocolos para asegurar las transacciones en línea son:**

- **El protocolo *HTTPS*** *(Hyper Text Transfer Protocol Secure).* Se trata de un protocolo que incrementa el nivel de seguridad de las páginas web.
- **Los certificados *SSL*** *(Secure Sockets Layer)* garantizan la autentificación, confidencialidad e integridad de los datos. Para conseguirlo el navegador cifrará esos datos.
- **El protocolo *SET*** *(Secure Electronic Transaction).* En este caso, se requiere de la instalación de un software tanto por parte del vendedor como del comprador. Permite hacer una transacción segura con independencia del tipo de red utilizada en la conexión.



El proceso de pago es una de las operaciones más sensibles en el comercio electrónico, por lo que se recomienda la utilización del requerimiento del código *CVV (card verifictaion value)* de las tarjetas. Con este código nos garantizamos que el ciberdelincuente que solamente tenga el número de la tarjeta no pueda utilizarla de forma fraudulenta. Otro mecanismo de verificación recomendado es el que permite comprobar que la dirección de facturación coincide con la dirección archivada en el banco emisor de la tarjeta de crédito.

IMPORTANTE

Transmitir seguridad en el comercio electrónico garantiza el aumento de la cartera de clientes.

PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 12/22

EL RGPD UE 2016/679 EN APLICACIÓN

Roles en la protección de datos: el delegado de protección de datos

Contenido

1. Roles en la protección de datos: el delegado de protección de datos.
2. Entidad inmobiliaria sancionada por no aplicar medidas de seguridad para proteger los datos personales.
3. ¿Cuáles son los principales consejos a seguir antes de realizar una compra en Internet?
4. Neurodatos y neurotecnología: privacidad y protección de datos personales.
5. ¿Cuáles son los ciberataques que puedo sufrir si tengo un comercio online?

La última de las figuras que vamos a tratar en este boletín, pero no por ello la menos importante, es el rol del delegado de protección de datos, en adelante (DPD).

En el Reglamento Europeo de protección de datos está regulada su designación, posición y funciones. En nuestra Ley Orgánica la LOPDGDD existe un Capítulo completo dedicado a regular la figura del DPD.

Podemos destacar la función que el DPD tiene como interlocutor del responsable o encargado de tratamiento ante la AEPD y las autoridades autonómicas de protección de datos. En este sentido el DPD podrá inspeccionar los procedimientos que aplique la entidad relacionados con la protección de datos y emitir recomendaciones.

Además, algo novedosos que supuso la entrada en vigor de la LOPDGDD, es que cuando la AEPD o la autoridad competente reciba una reclamación de un afectado, podrá hacerla llegar al DPD para que la resuelva en el plazo de un mes. De igual modo, cuando el responsable y encargado de tratamiento hubieran designado un DPD, el interesado podrá dirigir su reclamación ante el DPD y éste deberá resolver en el plazo máximo de dos meses.

IMPORTANTE

Se considera una infracción grave la falta de designación del DPD cuando su nombramiento sea exigible por la normativa de protección de datos.

SANCIONES DE LA AEPD

Entidad inmobiliaria sancionada por no aplicar medidas de seguridad para proteger los datos personales

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00404-2022.pdf, se sanciona a una entidad inmobiliaria con 3.500 €.

La reclamación fue interpuesta por una persona que estaba interesada en uno de los anuncios publicados por la inmobiliaria. En el escrito de reclamación alegaba que el correo electrónico que recibió con la respuesta de la entidad estaba visible las direcciones de correo electrónico de otras personas. Como prueba relevante se acompaña a la reclamación la copia del correo electrónico recibido.

La directora de la Agencia Española de Protección de Datos admitió a trámite la reclamación presentada. Se procedió a solicitar información a la parte reclamada, pero ésta no contestó al requerimiento.

La entidad fue sancionada con 2.000 € por incumplimiento de uno de los principios regulados en el RGPD, el principio de integridad y confidencialidad. Al enviar un correo electrónico sin utilizar la copia oculta se está vulnerando la confidencialidad de los datos del resto de destinatarios. **Por otro lado, además, se le sanciona con 1.500 € por no cumplir con la obligación de aplicar las medidas técnicas organizativas apropiadas que garantizasen un nivel de seguridad adecuado** con el tratamiento de los datos personales, tal y como dispone el art. 32 del RGPD.

Las actuaciones negligentes de los responsables y encargados de tratamiento pueden incumplir importantes preceptos del RGPD como ocurre en esta resolución.

IMPORTANTE

El responsable y el encargado del tratamiento deben determinar las medidas técnicas y organizativas adecuadas al tratamiento.

LA AEPD ACLARA

¿Cuáles son los principales consejos a seguir antes de realizar una compra en Internet?

En las fechas en las que nos encontramos se hace necesario tener herramientas y consejos claves para que las compras por Internet sean lo más seguras posibles. La AEPD junto con otros organismos, han elaborado una guía de Compra segura en Internet, en la que se recogen aspectos esenciales a tener en cuenta.

Así, por ejemplo, en la guía encontramos un apartado con las recomendaciones que debemos seguir antes de realizar una compra o contratar:

1º **Recomendaciones de seguridad básicas**: Confirmar que el sistema operativo del dispositivo, todos los programas y aplicaciones instaladas estén actualizadas con la última versión.

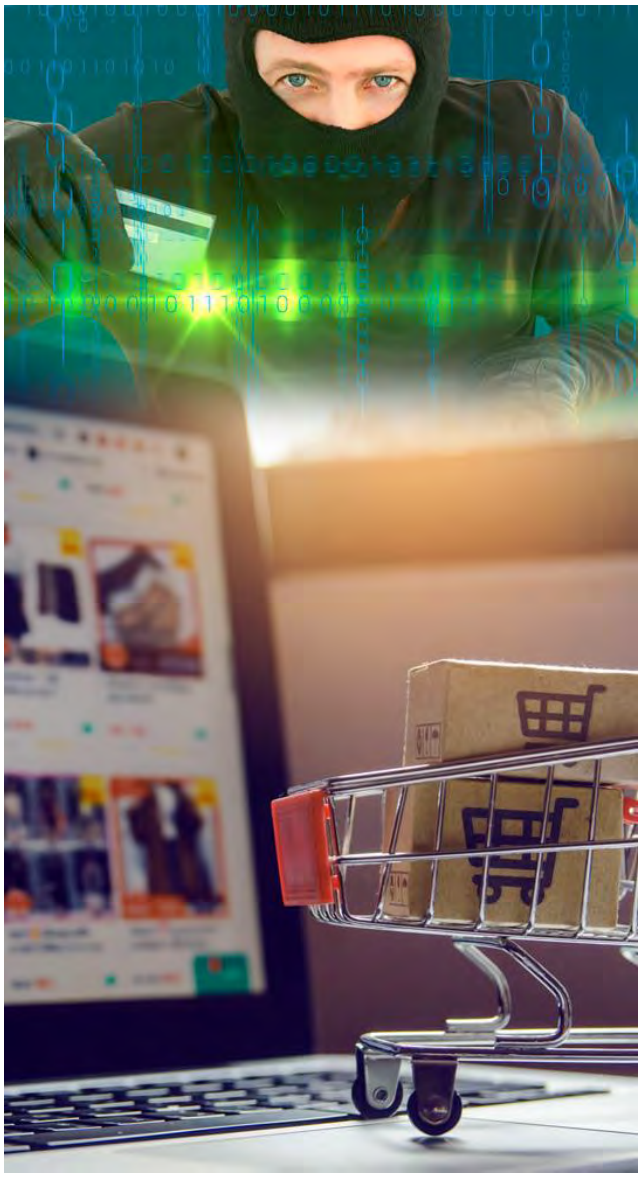
2º **Configuración de la red**: No conectar el dispositivo a una red *WiFi* pública para realizar transacciones de pago. Configurar adecuadamente el *WiFi* doméstico.

3º **Comprobar la información legal del comercio electrónico**: Aviso legal, Términos de uso, Política de privacidad y Condiciones generales de contratación.

4º **Verificar el titular y los datos del registro del dominio.** Comprobar si coincide con el que se identifica como responsable del sitio web.

5º **Comprobar que se tratan de comunicaciones seguras** (HTTPS).

6º **Sellos de confianza**: Los sellos de confianza dan fiabilidad y seguridad en los comercios electrónicos.



IMPORTANTE

Se recomienda sospechar de tiendas con precios por debajo del precio del mercado, sin información legal y el diseño web no transmita homogeneidad.

ACTUALIDAD LOPD

Neurodatos y neurotecnología: privacidad y protección de datos personales

Fuente: AEPD

Los recientes avances en neurotecnología e inteligencia artificial están permitiendo la aparición de un número creciente de dispositivos conectados que monitorizan la actividad cerebral para distintos propósitos. Estos dispositivos, ya disponibles en el mercado, y que se usan como accesorios portátiles con fines de entretenimiento o control de otros dispositivos, forman parte del conocido Internet de los Cuerpos (IoB, *Internet of Bodies*). Los datos cerebrales o neurodatos podrían identificar a los individuos, inferir estados emocionales, pensamientos o sentimientos, y revelar otras categorías especiales de datos.

Las interfaces cerebro-computador o BCI (*Brain Computer Interface*), son dispositivos que posibilitan la interacción directa entre el cerebro y un ordenador. Los BCI permiten interactuar con el mundo físico y virtual utilizando la mente. Para conseguirlo, recogen y miden las señales y la actividad del cerebro y con el software adecuado de captura y procesamiento, son capaces de extraer características de interés relacionadas con las intenciones y estado mental del usuario, y ejecutar acciones en consecuencia.

Aunque pueda parecer futurista, estamos hablando de tecnologías que ya están en el mercado de consumo. Grandes compañías (Snap, Valve, Meta, Apple, Samsung) están incorporando en sus productos tecnologías y dispositivos para captura de neurodatos.

Las primeras aplicaciones BCI tenían como objetivo proporcionar un canal de comunicación alternativo para usuarios con problemas de movilidad o del habla. Sin embargo, una serie de aplicaciones neuro-tecnológicas se ha abierto camino en el mercado y se ha integrado con un conjunto de dispositivos de consumo para usuarios sanos con diversos fines no clínicos. Estas aplicaciones buscan experiencias más inmersivas y completas en distintos usos (hogar inteligente, educación, neuromarketing, juegos y entretenimiento, internet, metaverso, seguridad y autenticación, ingeniería militar, etc).

Emotiv, Neurosky, Nextmind, OpenBCI, NexTem, Unicorn-bi, *Brainattach*, etc, ofrecen, a precios ya muy asequibles, un surtido de cascos inalámbricos para usarse en juegos y otras formas de entretenimiento, aplicaciones de marketing, monitorización o comunicación. Se comercializan también entornos de desarrollo software (incluso existen opciones de software libre) que facilitan la adquisición de datos recogidos por el BCI para desarrollar aplicaciones.

Puede ver más información en el siguiente enlace

Internet de los Cuerpos

Sección Innovación y Tecnología

EL PROFESIONAL RESPONDE

¿Cuáles son los ciberataques que puedo sufrir si tengo un comercio online?

Los comercios electrónicos están expuestos a una serie de ciberataques que ponen en peligro su reputación y actividad comercial. Es importante conocer cuáles son los principales para poder prevenirlos.

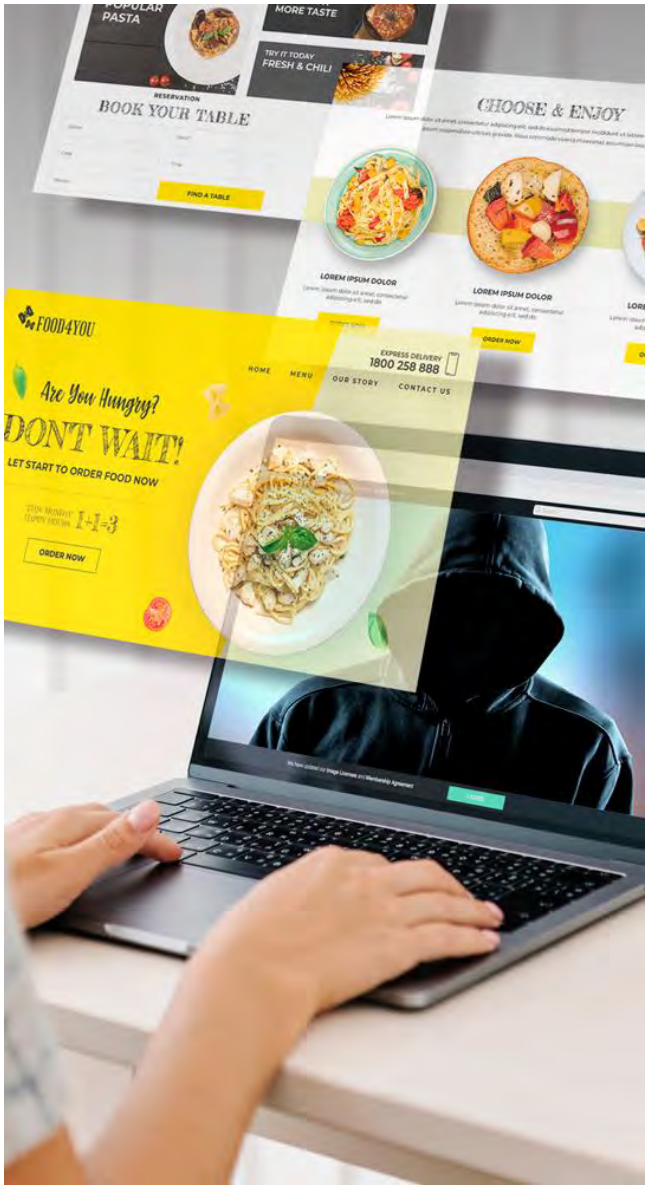
1º **El *defacement***: este ataque actúa sobre la apariencia visual de una página. Se reemplaza el sitio web alojado por uno propio, con el fin de cargar *malware* o eliminar archivos esenciales del servidor o dañar la imagen del comercio online. La mejor prevención en estos casos es incorporar una política de actualizaciones, una política de contraseñas seguras y realizar copias de seguridad periódicas.

2º **Ataque de denegación de servicio**: se puede bloquear la web y paralizar toda la actividad comercial. Para prevenir este tipo de ataques la entidad deberá aplicar elementos de protección perimetral.

3º **Bloqueo de acceso al panel de control** de la página web o servidor donde está alojado el comercio online.

4º **Infección por *malware*** cuando se utiliza en la página web software desactualizado o con vulneraciones no parcheadas.

Las recomendaciones para prevenir estos tipos de ataques entre otras, sería mantener actualizados los sistemas, realizar auditorías periódicas de seguridad y practicar la técnica de *egosurfing* que nos permite detectar campañas de suplantación a las entidades.



IMPORTANTE

La concienciación del personal laboral en materia de seguridad es una medida muy potente de seguridad.