RESUMEN
NOTICIAS DE ACTUALIDAD
EN PROTECCION DE DATOS
Y
BOLETINES "LA LOPD EN LA EMPRESA"
AÑO 2017

Un año más, a través del presente boletín trasladamos una exposición detallada de las noticias, actividades desarrolladas durante el año 2017 en materia de protección de datos de carácter personal, tratando de proporcionar una visión y orientación a nuestros clientes con respecto a la aplicación de dicha norma, a través de un examen del estado actual de la protección de los datos personales y el análisis de cómo se están afrontando los principales desafíos presentes y futuros, tanto en el ámbito nacional como en el supranacional. Le mostramos resumen de sanciones, inspecciones, noticias aparecidas en prensa, que muestran como en el día a día la LOPD se encuentra presente en prácticamente cualquier sector, siempre que se esté tratando con datos de carácter personal.

El presente Boletín Informativo tiene como finalidad servir de orientación a nuestros clientes respecto a la aplicación de la normativa de protección de datos. No pretendemos más que ampliar su conocimiento en protección de datos, mantenerle informado de actuaciones de la AEPD y transmitirles cualquier novedad que estimemos pueda ser de su interés. Esperamos haber contribuido mínimamente a tu planificación docente, quedando a tu disposición para cuantas consultas quieras realizarnos.

Las noticias a continuación expuestas son un exponente de la concienciación e interés que poco a poco esta legislación está alcanzando en España.

902. 15. 22. 25.
edorteam@edorteam.net / prodasur@prodasur.es
www.edorteam.net / www.prodasur.es

MEMORIA AEPD 2016:

Extractos de interés en estadísticas:

Atención al ciudadano.
Áreas con mayor importe global de sanciones.
Procedimiento Tutelas de derechos resueltas.
Inscripción de titularidad privada.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD 2016

La aplicación del nuevo Reglamento General de Protección de Datos, que entró en vigor el 25 de mayo de 2016 y que será aplicable dos años después, está definiendo en gran medida no sólo el futuro de este derecho fundamental sino también las actuaciones de esta Agencia.

El Reglamento va a requerir la adaptación tanto del marco regulatorio vigente como de los principales actores implicados (ciudadanos, responsables y profesionales de la privacidad). La Agencia, como institución que tiene encomendada la garantía de proteger los datos de los ciudadanos, también ha puesto en marcha medidas para afrontar los cambios próximos y facilitar a estos actores, cada uno con sus peculiaridades, la transición a la nueva normativa.

La Agencia considera imprescindible afianzarse como un organismo colaborador y transparente que actúe de la manera más ágil y eficaz posible, a la vez que apostar por la concienciación en la doble vertiente antes mencionada: la de los ciudadanos, para que sean conscientes de qué derechos les amparan y cómo ejercitarlos, y la de aquellos que tratan datos, que deben abordar este asunto como un valor añadido que puede contribuir a su crecimiento y a una mejora de su competitividad. Las vías puestas en marcha para lograrlo convergen en una única finalidad: conseguir la protección efectiva de unos ciudadanos que, como indican todos los estudios, están cada vez más preocupados por la utilización de sus datos personales.

Las consultas recibidas en el área de Atención al Ciudadano han superado las 236.000, un incremento del 8% que se suma al 10% que ya se había producido en 2015 sobre 2014. A este respecto, hay que destacar que buena parte de las consultas ciudadanas más frecuentes están relacionadas con la inclusión indebida en ficheros de morosidad, una materia que, por otro lado, también es una de las principales fuentes de reclamaciones planteadas ante la Agencia. Junto con la contratación irregular de servicios, supone el grueso de las denuncias que recibe cotidianamente la Agencia, y de ahí que se haya optado por darles un tratamiento singularizado en el apartado de cifras de esta Memoria.

En cuanto a denuncias y reclamaciones, la Agencia ha recibido más de 10.500 en 2016. Las primeras se han reducido con respecto a 2015 un 6,5%, si bien las reclamaciones de tutela se han incrementado un 24,3%. En este punto es necesario mencionar que esta institución ha acometido una profunda reorganización interna que tiene como finalidad la tramitación ágil a la vez que rigurosa de los temas planteados.

Además de la actividad generada por las consultas, denuncias y reclamaciones planteadas por los ciudadanos, las cuestiones atendidas por el Gabinete Jurídico y la inscripción de ficheros, el año que recoge esta Memoria ha destacado por el incremento de las solicitudes de transferencia internacional de datos presentadas y concedidas con motivo de la sentencia del Tribunal de Justicia de la Unión Europea que declaró inválida la Decisión de Puerto Seguro.

Estas y otras cifras, que se desglosan de manera pormenorizada en las siguientes páginas, así como el análisis de otras iniciativas menos susceptibles de cuantificación, ponen de manifiesto sin ninguna duda la creciente importancia que la protección de datos ha adquirido en la sociedad actual y la indudable apuesta que se ha de realizar para mantener el nivel de protección que nos hemos otorgado. Para finalizar, debo reconocer la labor desempeñada por el personal de todos los departamentos de la Agencia, una plantilla cuyo número se mantiene intacto desde 2008 y que, sin embargo, asume un número cada vez mayor de tareas más complejas y se enfrenta a nuevos retos derivados de la implementación del Reglamento.

Mar España Martí

Directora de la Agencia Española de Protección de Datos

MEMORIA 2016

ATENCIÓN AL CIUDADANO

CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO

	ATENCIÓN PRESENCIAL	TELÉFONO	POR ESCRITO	SEDE ELECTRÓNICA	RESPUESTA AUTOMÁTICA FAQs	TOTAL
AÑO 2014	3.361	89.868	592	5.703	97.854	197.378
AÑO 2015	3.767	74.260	550	7.054	132.704	218.335
AÑO 2016	4.183	76.869	552	8.054	147.297	236.955
INCREMENTO 2015-2016	**11,04%**	**3,51%**	**0,36%**	**14,17%**	**10,99%**	**8,52%**

ÁREAS CON MAYOR IMPORTE GLOBAL DE SANCIONES

ACTIVIDAD	2014 (€)	2015 (€)	2016 (€)	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
Ficheros de morosidad			**5.835.007**	45,85		
Contratación fraudulenta			**3.420.003**	26,88		
Publicidad (excepto *spam*)	751.411	502.108	**1.964.305**	15,44	291,21	161,42
Telecomunicaciones	10.750.502	7.090.004	**549.800**	4,32	–92,25	–94,89
Entidades financieras	2.018.501	2.395.902	**516.001**	4,06	–78,46	–74,44
Comunicaciones electrónicas comerciales – *spam* (LSSI)	645.506	897.403	**439.851**	3,46	–50,99	–31,86
TOTAL (6 PRIMERAS)	**14.165.920**	**10.885.417**	**12.724.967**	**100,00**	**16,90**	**–10,17**
% RELATIVO AL TOTAL DEL AÑO	**83,32%**	**79,38%**	**89,67%**		**12,97**	**7,62**

MEMORIA 2016

PROCEDIMIENTOS DE TUTELA DE DERECHOS

DISTRIBUCIÓN DE DERECHOS TUTELADOS SEGÚN RESULTADO DE LA RESOLUCIÓN

	ESTIMATORIA	ESTIMATORIA FORMAL O PARCIAL	DESESTIMATORIA	TOTAL
Cancelación	201	143	268	612
Acceso	123	94	122	339
Rectificación	10	11	15	36
Oposición/exclusión	37	22	28	87
TOTAL	371	270	433	1.074

En cada procedimiento resuelto puede haberse tutelado más de un derecho ARCO.

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN TERRITORIAL DE FICHEROS

	RESPONSABLES		FICHEROS	
	2016	TOTAL	2016	TOTAL
Comunidad Autónoma de Andalucía	**38.652**	**223.762**	**96.922**	**697.748**
Almería	3.903	20.791	9.678	68.467
Cádiz	5.086	28.571	13.734	90.252
Córdoba	3.929	20.781	10.053	65.396
Granada	5.302	29.664	12.944	96.047
Huelva	1.421	9.666	3.293	28.748
Jaén	2.606	16.734	7.107	57.441
Málaga	8.297	50.942	22.832	159.255
Sevilla	8.146	47.511	17.281	132.142

NOTICIAS DE PRENSA DE INTERÉS EMITIDAS EN 2017

26/01/2017. La AEPD presenta nuevos materiales para ayudar a las pymes a cumplir con el Reglamento europeo de Protección de Datos. FUENTE: agpd.es

La AEPD presenta nuevos materiales para ayudar a las pymes a cumplir con el Reglamento europeo de Protección de Datos

La Agencia quiere facilitar que, durante este periodo transitorio, las pymes puedan conocer el impacto que va a tener el Reglamento en la forma en la que tratan datos y las medidas que deben adoptar.

El Reglamento europeo de Protección de Datos entró en vigor el 25 de mayo de 2016 y será de obligatorio cumplimiento el 25 de mayo de 2018

Los nuevos materiales incluyen una 'Guía del Reglamento para responsables', 'Directrices para elaborar contratos entre responsables y encargados', y una 'Guía para el cumplimiento del deber de informar', todos ellos incluidos en una nueva sección web específica

Los recursos han sido elaborados por la Agencia Española, la Autoridad Catalana y la Agencia Vasca de Protección de Datos

Madrid, 26 de enero de 2017. La Agencia Española de Protección de Datos (AEPD) ha publicado hoy nuevos materiales y recursos con los que facilitar a las pequeñas y medianas empresas su adaptación al Reglamento General de Protección de Datos (RGPD), que entró en vigor el 25 de mayo de 2016 y comenzará a aplicarse el 25 de mayo de 2018. Los materiales incluyen una ''Guía del Reglamento para responsables de tratamiento'', ''Directrices para elaborar contratos entre responsables y encargados'' y una ''Guía para el cumplimiento del deber de informar'', todos ellos elaborados junto a la Autoridad Catalana y la Agencia Vasca de Protección de Datos.

La Agencia, en su faceta preventiva, quiere facilitar que, durante este periodo transitorio, las pymes conozcan el impacto que va a tener el Reglamento en la forma en la que tratan datos para que puedan adaptar sus procesos a la nueva normativa, ya que esta supone un cambio en el modelo de cumplimiento y exige un compromiso más activo. El objetivo es ofrecer la mayor información posible a las pymes, que suponen el 99% del tejido empresarial español. Los materiales presentados hoy son los siguientes:

- Guía del Reglamento General de Protección de Datos para responsables de tratamiento. El documento recoge las principales cuestiones que las organizaciones deben tener en cuenta para cumplir con las obligaciones recogidas en el Reglamento. La Guía incluye en su parte final una Lista de verificación con la que las entidades pueden determinar si han dado los pasos necesarios para estar en condiciones de hacer una correcta aplicación del RGPD. Guía del Reglamento General de Protección de Datos para responsables de tratamiento

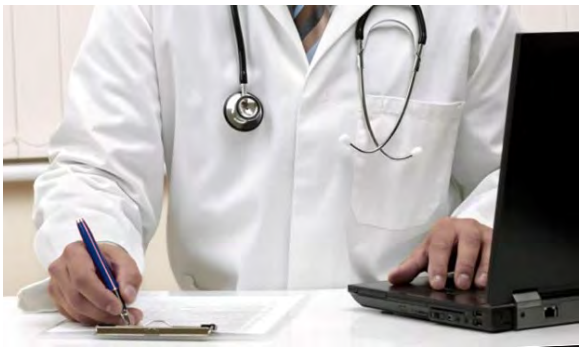
Algunas de las recomendaciones que se ofrecen en la Guía pueden ponerse en práctica de forma casi inmediata, porque tienen que ver con actuaciones que debieran iniciarse ya durante este periodo transitorio. En otros casos, esas recomendaciones o propuestas solo deberán tenerse en cuenta en el momento en que el RGPD sea de aplicación, aunque se han incluido para fomentar que las entidades puedan ir anticipándose al momento en el que las medidas sean de obligado cumplimiento.

-Directrices para la elaboración de contratos entre responsables y encargados de tratamiento . El RGPD establece que las relaciones entre el responsable y el encargado deben formalizarse en un contrato o acto jurídico que les vincule, regulando de forma minuciosa su contenido mínimo. Estas directrices se han realizado con la finalidad de que los contratos reflejen todos los contenidos recogidos en el Reglamento.

- Guía para el cumplimiento del deber de informar. El RGPD concede gran importancia a la información que debe proporcionarse a los ciudadanos cuyos datos van a tratarse, estableciendo una lista exhaustiva de los contenidos que deben ser expuestos de forma clara y accesible. Esta Guía ofrece recomendaciones y soluciones prácticas sobre los modos de proporcionar esta información.

Estos recursos están incluidos en una nueva sección web específica sobre el Reglamento, que también incorpora otros elementos que pueden resultar útiles para que las entidades puedan adaptarse de forma paulatina al RGPD. La AEPD, por otro lado, se encuentra preparando una herramienta de autoevaluación online dirigida a favorecer que pequeñas y medianas empresas puedan valorar de forma rápida y sencilla si sólo realizan tratamientos que en principio plantean un bajo o muy bajo riesgo para los derechos de los interesados, y ofrecerles el acceso a las medidas de cumplimiento que el Reglamento Europeo exige en estos casos.

12/02/2017. Estas son las seis formas más comunes de que un médico se salte la ley. FUENTE: redaccionmedica.com



Estas son las seis formas más comunes de que un médico se salte la ley

La llegada de las nuevas tecnologías hace que numerosos profesionales infrinjan las leyes de protección de datos

Las nuevas tecnologías han abierto un amplio elenco de posibilidades en la relación médico-paciente, pero también suponen un desafío.

Numerosos profesionales médicos incurren en prácticas prohibidas por la ley en materia de protección de datos. Las nuevas tecnologías han abierto un amplio elenco de posibilidades en la relación médico-paciente, pero también suponen un desafío, ya que muchos de estos sistemas no garantizan adecuadamente la protección de datos. Así lo cree al menos el psiquiatra Josep María Fábregas que, sin entrar en aspectos regulados por la deontología profesional y simplemente basándose en el código penal identifica seis conductas dudosas. “Es fundamental que los profesionales médicos nos dotemos de herramientas o plataformas que permitan el intercambio de datos personales con total seguridad”, explica Fábregas, quien impulsa su propia ‘app’ de intercambio de datos seguro.

Videoconferencias por Skype

Algunos profesionales médicos que se anuncian por Internet y ofrecen como herramienta principal de comunicación la videoconferencia online a través de esta plataforma. Por sus características, Skype resulta un medio intuitivo y ágil para que el médico pueda atender a su paciente. Ahora bien, su política de privacidad no es perfecta y nadie asegura que el contenido que se comparte esté completamente guardado en el anonimato.

Envío de informes a través del correo electrónico

El email es ya el canal de comunicación clásico para el intercambio de archivos, también en materia de salud. Sin embargo, los servidores tampoco pueden asegurar que la información que circula a través de ellos se mantenga de forma anónima, por lo que enviar a través de correo electrónico un informe médico

Archivo de datos en ordenadores o dispositivos móviles personales.

Descargarse una documentación de un paciente, a través de Internet, al ordenador personal o smartphone, se considera archivo ilegal de datos personales.

Envío de datos a través de Whatsapp

Las aplicaciones que permiten el intercambio de mensajes instantáneos son realmente una herramienta útil en caso de urgencia, pero no parece ser el canal más seguro que existe para intercambiar información personal.

Compartir información en las redes sociales.

Lugares como Facebook o Twitter no son los idóneos para compartir datos de pacientes. Evidentemente no lo es el ‘timeline’. Pero tampoco los mensajes personales que permiten enviar estas aplicaciones. Un simple hackeo de la contraseña del usuario o robo del dispositivo y datos muy sensibles pueden quedar expuestos.

Consultas online

Si el profesional tiene una página web personal o plataforma médica online donde realiza la actividad con sus pacientes, obviamente tendrá que reunir todos los protocolos de seguridad para asegurar la confidencialidad de los datos.

21/02/2017. Las transferencias internacionales de datos personales y el reto de salvaguardar los derechos fundamentales de los afectados. FUENTE: elderecho.com

Las transferencias internacionales de datos personales y el reto de salvaguardar los derechos fundamentales de los afectados

Recientemente, la polémica generada por el denominado “Caso Schrems” o “Caso Facebook”-enmarcado en el litigio iniciado por el estudiante y activista austriaco Maximilliam Schrems contra Facebook Ireland Ltd., por considerar que las transferencias internacionales de datos personales que dicha entidad realizaba a Estados Unidos no garantizaban un nivel adecuado de protección sobre sus derechos- contribuyó a fijar el foco de atención sobre los movimientos internacionales de datos. Asimismo, obligó a que las autoridades europeas se replanteasen la eficacia de algunas de las bases jurídicas que hasta entonces articulaban su regulación, especialmente después de que el Tribunal de Justicia de la Unión Europea (TJUE) declarase inválida mediante Sentencia de 6 de octubre de 2015 (asunto C-362/14), la Decisión 2000/520/CE, de la Comisión, de 26 de julio de 2000, que consideraba a Estados Unidos como un Puerto Seguro (Safe Harbour) en relación a las transmisiones internacionales de datos de carácter personal con destino a este país.

La sentencia dictada por el TJUE, implicó renegociar las condiciones en materia de privacidad y seguridad de datos que debían regir en las transferencias internacionales UE-EEUU, con el fin de neutralizar cualquier posible riesgo que aquellas pudieran suponer para la protección de la vida privada, los derechos y las libertades fundamentales de los titulares de los datos personales. Sin embargo, las consecuencias derivadas del “Caso Schrems” son únicamente un ejemplo dentro de las múltiples garantías que ya se venían exigiendo a la hora de realizar esta clase de movimientos internacionales de datos.

Si nos atenemos al concepto estricto de transferencia internacional, esta supondría que un exportador de datos (responsable o encargado del tratamiento) situado en el Espacio Económico Europeo (EEE), efectuase una transmisión de datos de carácter personal con destino a un importador de datos (responsable, encargado o subencargado del tratamiento) situado en un tercer país, el cual no necesariamente ha de estar en condiciones de garantizar un nivel adecuado de protección para el tratamiento de los datos personales objeto de la transmisión.

En caso de que dicho nivel de protección no pueda ser garantizado, los riesgos para la seguridad de los datos personales transferidos, y en consecuencia, para la protección de la vida privada de los afectados, pueden llegar a ser muy elevados. Es por ello, que tanto la regulación en el ámbito europeo, a través de la Directiva 95/46/CE, como en el ámbito nacional mediante la propia Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), su reglamento de desarrollo, y la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos, han intentado configurar un marco jurídico exigente respecto a las garantías a adoptar por los operadores de las transferencias internacionales de datos. En

relación a los requisitos exigidos en materia de transferencias internacionales, podríamos distinguir tres supuestos fundamentales a tomar en consideración:

1.- Que la transferencia internacional tenga como destinatario a un importador que se encuentra en un tercer país, respecto al cual la Comisión Europea ha declarado que ofrece un nivel adecuado de protección.

Actualmente, la Comisión Europea ha decretado un nivel adecuado de protección, respecto a Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Estados Unidos. En el caso particular de Estados Unidos, la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EEUU, ha sentado las nuevas bases jurídicas aplicables a las transferencias realizadas con destino a Estados Unidos, tras el impacto ocasionado por el reseñado "Caso Schrems" y la sentencia dictada a este respecto por parte el TJUE. El Escudo de privacidad proporciona una lista con las entidades certificadas como Puerto Seguro y por tanto, respecto a las cuales se consideraría que aportan o garantizan un nivel adecuado de protección.

2.- Que la transferencia internacional tenga como destinatario un importador situado en un tercer país, respecto al cual la Directora de la Agencia Española de Protección de Datos (AEPD) estime que presenta un nivel adecuado de protección, a la luz de las normas vigentes en dicho Estado, y tras realizar una evaluación sucinta de aspectos tales como la naturaleza de los datos, la finalidad del tratamiento, la duración del mismo, o las medidas de seguridad aplicables y que se encuentren en vigor tanto en el país de origen como en el país de destino de la transferencia de datos personales. Además, ha de tenerse en cuenta que el nivel de protección exigido debe ser equiparable o recíproco al proporcionado por las disposiciones, exigencias y obligaciones fijadas por la LOPD y su reglamento de desarrollo.

Es preciso señalar, que en cualquiera de los dos casos precedentes, será necesario proceder a la notificación de la transferencia internacional frente a la AEPD y a su consiguiente inscripción en el Registro General de Protección de Datos (RGPD). Complementariamente, en caso de que las relaciones entre el exportador y el importador impliquen un acceso a datos personales derivado de la prestación de un servicio -en los términos fijados por el artículo 12 de la LOPD-, será igualmente necesario suscribir un contrato de encargo de tratamiento de datos personales, siendo por supuesto de obligado cumplimiento el resto de disposiciones de la LOPD y su reglamento de desarrollo.

3.- Que la transmisión de datos personales tenga como destinatario un importador situado en un tercer país que no ofrece un nivel adecuado de protección, y que dicha transmisión de datos no se encuadre en ninguno de los supuestos excepcionados en virtud del artículo 34 de la LOPD. Entre dichas excepciones, se encontrarían por ejemplo, las transferencias realizadas con consentimiento del afectado o aquellas cuya finalidad sea el ejercicio, reconocimiento o defensa de un derecho en el marco de un proceso judicial.

Por tanto, en aquellos supuestos en los cuales el nivel de seguridad y protección aportado por el Estado o país de destino -respecto a los datos personales afectados- sea suficiente o adecuado, y no podamos acudir a las excepciones recogidas por el artículo 34, deberemos acudir a la regla general fijada por el artículo 33 de la LOPD, que impone la necesidad de obtener una autorización por parte de la Directora de la AEPD. Dicha autorización será preceptiva para poder llevar a cabo la transmisión internacional de datos, y de hecho, la elusión de este requisito obligatorio constituirá una infracción de carácter muy grave, tal y como prevé el artículo 44.4.d) de la LOPD.

Para que la autorización pueda ser otorgada, se deberán aportar garantías suficientes que permitan asegurar la salvaguarda y protección de la vida privada, los derechos y libertades fundamentales, de los titulares de los datos personales afectados. La forma más idónea para aportar dichas garantías, será la suscripción de un contrato entre el exportador y el importador de datos, en el cual se podrán emplear -con el fin de suplir las posibles deficiencias que presentase la transferencia- las denominadas Cláusulas Contractuales Tipo.

En virtud de si la transferencia se da entre dos responsables del tratamiento, entre un responsable y un encargado del tratamiento, o entre un encargado situado en territorio español y un subencargado del tratamiento, las Cláusulas Contractuales

Tipo a utilizar para suscribir los contratos experimentarán variaciones, tal y como se refleja a continuación:

a) Así pues, para el primer caso, serán aplicables las Cláusulas Contractuales Tipo previstas en la Decisión de la Comisión Europea 2001/497/CE, de 15 de junio de 2001, y la Decisión 2004/915/CE, de 27 de diciembre de 2004, debiendo el exportador y el importador optar en bloque únicamente por uno de los dos conjuntos de cláusulas.

b) Para el segundo supuesto, se aplicarán las cláusulas contenidas en la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero de 2010, además de lo dispuesto en la norma sexta de la Instrucción 1/2000 de la AEPD y en el artículo 12 de la LOPD, puesto que al estar ante un tratamiento de datos por cuenta del responsable del fichero o tratamiento, deberán hacerse constar en el contrato las obligaciones atribuidas al encargado del tratamiento. Dichas obligaciones harán especial referencia al seguimiento de las instrucciones aportadas por el responsable del tratamiento, a la devolución o destrucción de los datos una vez finalizada la prestación del servicio que vincula a ambas partes, y a las medidas de seguridad que aquél deberá adoptar respecto a los datos personales, que no serán otras que las exigidas al exportador conforme a la legislación española en materia de protección de datos.

c) Finalmente, para el tercer supuesto se podrán incluir en el contrato a suscribir por ambas partes, las cláusulas adoptadas por la Agencia Española de Protección de Datos, en su resolución de Autorización de Transferencia Internacional de Datos de 16 de octubre de 2012. Complementariamente, se requerirá además la suscripción de un acuerdo entre el responsable y el encargado del tratamiento, en virtud del

cual se autoricen tanto la contratación del subencargado del tratamiento, como la realización de la transferencia internacional. Se articularía en este supuesto una doble relación a regular y acreditar, que vincula por una parte a responsable y encargado, y por otra, a encargado y subencargado. A pesar de que esta última relación sería la realmente relevante a la hora de efectuar la transferencia internacional, ha de incardinarse necesariamente en el contrato-relación marco entre el responsable y el encargado del tratamiento.

Por último, una vez señalados los tres principales supuestos a los que aplicar las denominadas Cláusulas Contractuales Tipo, mención aparte requerirían las denominadas Binding Corporate Rules (BCR). Las BCR o reglas corporativas vinculantes, son normas internas a adoptar e implementar por las empresas pertenecientes a un mismo Grupo, entre las cuales vaya a tener lugar una transferencia internacional de datos personales. La estructura, los elementos y requisitos que han de tener las BCR han sido específicamente abordados por el Grupo de Trabajo del Artículo 29 -también conocido como GT29- en calidad de órgano consultivo independiente creado por la Directiva 95/46/CE. Este sistema podría resultar eficaz para los supuestos de transmisión de datos personales, por ejemplo, entre las sedes de las empresas multinacionales que se hallen establecidas en la UE y su matriz en EEUU, lo cual sucede en el caso de la mayor parte de las grandes multinacionales del sector tecnológico, incluidas empresas como Facebook o Google.

22/02/2017. ¿Pueden colegios o padres publicar fotos de actividades de sus hijos en la red? FUENTE; elconfidencial.com

¿Pueden colegios o padres publicar fotos de actividades de sus hijos en la red?

La publicación de fotografías de menores de 14 años está supeditada al permiso de los padres, en caso contrario se vulnerarán los derechos del propio niño recogidos por la ley

Mi hijo de 11 años tuvo una función de teatro en el cole, en la que iban todos los niños de la clase disfrazados por carnaval, yo llevé mi cámara y publiqué las fotos en mi Facebook y mi Instagram. Tengo la configuración en 'privado', pero para mi sorpresa, me ha llegado una carta del colegio diciendo que un padre no quiere que ni su hijo ni él mismo salgan en ninguna fotografía, este padre es, obviamente, el padre de uno de los niños y resulta que los padres están divorciados y él no ha dado su permiso para las fotos. Mi pregunta es: ¿no puedo colgar las fotos de mi hijo por miedo a que salga este otro niño? Si mi cuenta es privada, no podrían saber si sale su hijo.

Como reflexión inicial, debemos saber que, ante este tipo de situaciones que se refieran a menores de 14 años, estas imágenes no podrán ser difundidas si al menos uno de los progenitores no da el consentimiento para que su hijo sea fotografiado, y posteriormente, publicada esa fotografía en cualquier medio.

En este caso concreto, por el hecho de estar los padres divorciados, debería, para mayor seguridad, existir el consentimiento de ambos en función de lo señalado en el Real Decreto 1720/2007 sobre protección de datos de carácter personal, que

señala claramente que “en el caso de los menores de 14 años se requerirá el consentimiento de los padres o tutores”.

En resumen, la representación legal de los hijos menores de edad la ostentan ambos progenitores; no obstante, en lo que se refiere a la patria potestad, se ejercerá conjuntamente por ambos progenitores o por uno solo con el consentimiento expreso o tácito del otro, siendo válidos los actos que realice uno de ellos conforme al uso social y a las circunstancias o las situaciones de urgente necesidad, y, en caso de desacuerdo, cualquiera de los dos podrá acudir al juez, quien, después de oír a ambos y al hijo, si tuviera suficiente juicio y fuera mayor de 12 años, decidirá qué progenitor tendrá la facultad, sin que su decisión pueda ser recurrida.

¿Puede mi expareja publicar fotos de nuestro hijo sin mi permiso en Facebook?

Publicar la vida de los hijos en redes sociales es cada día más habitual para deleite de familiares y allegados. Sin embargo, se trata de una conducta no exenta de riesgo

En cuanto a la publicación en nuestra red social, ya sea Facebook, Instagram o cualquier otra, con independencia de que la configuración de la misma sea privada (solo podrán acceder a estas fotos aquellas personas que tengan nuestro consentimiento) o pública, también necesitaríamos el permiso expreso de los padres o tutores de todos los menores que sean identificables en la foto. Nuestra recomendación sería tener ese consentimiento por escrito, recordando además que este consentimiento puede ser revocado en cualquier momento.

La imagen de una persona, sea adulto o menor, se considera un dato de carácter personal, puesto que permite identificar a una persona. Esto viene recogido en el artículo 3 de la LOPD, y por lo tanto se trata de un dato protegido por esta ley y por las regulaciones que la desarrollan. Además, la Ley Orgánica 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen también establece que el derecho al honor, a la intimidad personal y familiar y a la propia imagen es irrenunciable, inalienable e imprescriptible.

En el mismo sentido, para la publicación en la web del colegio o en la revista de este, sería necesario también el consentimiento de los padres o tutores, como resumen en el Gabinete Jurídico de la Agencia Española de Protección de Datos: “La publicación en la página web del colegio de las fotos de los alumnos constituye una cesión o comunicación de datos de carácter personal, definida por el artículo 3 j) de la LOPD como toda revelación de datos realizada a una persona distinta del interesado. En consecuencia, tanto la toma de las fotografías como su publicación en internet requieren el consentimiento, en los términos antes señalados, del afectado o de sus padres si se trata de un menor de 14 años, de forma que cuando se tratan y ceden dichos datos personales sin el pertinente consentimiento, la LOPD establece el correspondiente mecanismo reactivo, constituido por el derecho de cancelación de datos de carácter personal, recogido en su artículo 16”.

Además, debemos recordar que la propia Agencia de Protección de Datos ha publicado unas recomendaciones para la protección de datos de los menores, en las que se señala que deben extremarse las precauciones en internet y, en particular, se indica que “no es aconsejable publicar fotos que identifiquen a un niño, por ejemplo, situándole en el contexto de un colegio y/o actividad determinados”.

23/02/2017. La AEPD publica la guía ‘Protección de datos y administración de fincas. FUENTE: agpd.es

La AEPD publica la guía 'Protección de datos y administración de fincas' para facilitar a este sector el cumplimiento de la normativa

El tratamiento de datos personales en el ámbito de las comunidades de vecinos constituye uno de los motivos de consulta más frecuentes ante la Agencia.

La información sobre comunidades de propietarios es uno de los temas más consultados en el catálogo de preguntas frecuentes de la página web de la Agencia

Esta guía forma parte del conjunto de iniciativas adoptadas por la Agencia para facilitar y fomentar el cumplimiento de la normativa de protección de datos.

El documento recoge la aplicación práctica de la normativa de protección de datos vigente, incorporando referencias al Reglamento General de Protección de Datos, que será aplicable a partir del 25 de mayo de 2018

(Madrid, 23 de febrero de 2017). La Agencia Española de Protección de Datos (AEPD) ha publicado la guía 'Protección de datos y administración de fincas', un documento que forma parte del conjunto de iniciativas adoptadas por la Agencia para facilitar y fomentar el cumplimiento de la normativa de protección de datos.

La información referente a comunidades de propietarios es uno de los temas más consultados en el catálogo de preguntas frecuentes de la página web de la Agencia. La AEPD considera que publicar una guía orientada a abordar la protección de datos en las comunidades de vecinos a través de los administradores de fincas contribuye tanto a facilitar el trabajo de estos, ofreciéndoles una información ajustada a sus necesidades, como a mejorar el nivel global de protección de los ciudadanos. Según datos del Consejo General de Colegios de Administradores de Fincas, estos gestionan el 80% del parque total de viviendas en España.

'Protección de datos y administración de fincas' aborda en primer lugar cuestiones generales de la normativa de protección de datos que se aplican a los administradores de fincas, que actúan por cuenta de las comunidades de propietarios. En este sentido, se incluyen secciones dedicadas a las definiciones de conceptos básicos, a la inscripción de ficheros y el futuro registro de actividades, a la forma de organizar las relaciones entre la comunidad de propietarios y el administrador, y a las principales obligaciones de las partes.

Por otro lado, la guía analiza con detalle algunos supuestos específicos que se plantean con frecuencia ante la Agencia, tanto en forma de consulta como de

denuncia: información sobre propietarios con pagos pendientes (publicación en el tablón de avisos de la finca de la identidad de los propietarios deudores y/o de las cuotas vencidas e impagadas), acceso y obtención de copias de la documentación de la comunidad, requisitos para la instalación de cámaras de videovigilancia o tratamiento de datos de empleados.

Aplicación del nuevo Reglamento europeo

El documento recoge la normativa de protección de datos vigente, incorporando también referencias al Reglamento General de Protección de Datos, que será aplicable a partir del 25 mayo de 2018 y que supone una gestión distinta de la que se realiza en la actualidad.

Esta guía puede complementarse con directrices y materiales adicionales destinados a apoyar a las entidades en su adaptación a la nueva normativa. Algunos de ellos pueden ser ya consultados y utilizados por las empresas, incluido el colectivo al que va dirigida esta guía. Así, la Agencia ha publicado recientemente la Guía del Reglamento europeo para responsables de tratamiento, la Guía para el cumplimiento del deber de información y la Guía para la elaboración de contratos entre responsables y encargados. Todas ellas están disponibles en la página web de la AEPD y pueden proporcionar un apoyo útil como complemento a esta guía y de cara al futuro marco normativo.

Por otra parte, 'Protección de Datos y administración de fincas' es la primera de una serie de guías sectoriales que va a publicar la Agencia a lo largo de 2017, y que abordarán, entre otras materias, el tratamiento de datos en centros docentes, la videovigilancia o la presentación de quejas y reclamaciones en el ámbito de las telecomunicaciones. En cualquier caso, la Agencia Española efectuará una revisión de esta guía para adaptarla plenamente al nuevo Reglamento Europeo en los meses anteriores a su efectiva aplicación.

23/03/2017. Una imagen vale más que mil palabras para justificar un despido. FUENTE: elmundo.es

Una imagen vale más que mil palabras para justificar un despido. La empresa sólo tendrá que informar de que ha instalado unidades de filmación.

Las imágenes tomadas por cámaras de videovigilancia servirán como prueba para despedir a un trabajador. No será necesario tener el consentimiento explícito del empleado para la grabación

Las grabaciones efectuadas por las cámaras de videovigilancia en el lugar de trabajo son ya una prueba fehaciente en los tribunales de lo Social para causas de despido. Si bien en el año 2000 una sentencia del Tribunal Constitucional (TC) ratificó la validez de este medio como prueba, cada caso planteado desde entonces ha dado pie a diferentes interpretaciones y a resoluciones judiciales dispares. No obstante, la coincidencia en los últimos meses de dictámenes en los que se ha aceptado como demostración válida de causa de despido las imágenes registradas por una cámara de seguridad han instado al Supremo a resolver que era preciso unificar la doctrina.

El último fallo del pleno del Tribunal Supremo, a instancias de una defensa realizada desde el despacho de abogados Grupo Gispert, en Barcelona, va más allá y no sólo resuelve un caso, sino que además establece como criterio definitivo que las imágenes obtenidas con una videocámara instalada en un lugar de trabajo son válidas como prueba para encausar a un empleado, a pesar de que éste no haya dado su consentimiento explícito para la grabación. Basta que, como indicó en su momento el TC al flexibilizar los requisitos, los trabajadores y sus respectivos representantes laborales hayan sido informados de la presencia de las unidades de filmación y de su ubicación -a modo orientativo- por la simple existencia de los carteles correspondientes.

Es decir, no se precisa ni un documento que acredite el consentimiento expreso del empleado a ser grabado, ni trasladar por escrito la información sobre la instalación de cámaras. Se da por supuesto que, en el ámbito laboral, nunca se precisa un consentimiento expreso porque el propio Estatuto de los Trabajadores determina en su artículo 20 que "el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso", observa Santiago Farré, jefe de la asesoría jurídica de la Autoridad Catalana de Protección de Datos.

Precedente importante

En opinión de Isaac González abogado laboralista del Grupo Gispert, y quien recurrió las resoluciones de despido improcedente, la sentencia establece un precedente importante para el uso que puedan hacer las empresas de las grabaciones de cámaras de videovigilancia: "Si el trabajador conoce que existen dispositivos que están en funcionamiento y su ubicación, debe saber que a partir de ahora los tribunales tendrán en cuenta esas grabaciones como medio de prueba en el caso de que se produzca un acto ilícito por su parte sin que con ello se vulneren sus derechos fundamentales".

Hasta ahora, las imágenes registradas en los centros de trabajo eran "una prueba diabólica", manifiesta el abogado González, porque dejaban al demandante, principalmente el empresario, "en una situación de indefensión" ante hechos que pueden considerarse faltas graves, como el hurto o la manipulación de las existencias, por ejemplo. La validez de la prueba se ponderaba a través «del juicio de proporcionalidad y de la idoneidad de su utilización, porque se vulnera el derecho a la intimidad» que establece la ley de protección de datos, señala Miguel Gudín, socio del despacho Glegal y profesor de la escuela de negocios OBS, y añade que de ahí la importancia también de la sentencia del Supremo, porque determina que cualquier cámara de vigilancia con filmaciones de espacios amplios usadas básicamente para controles de seguridad es válida para tomar medidas disciplinarias versus un empleado. «Es un cambio importante ¿Justo o no? Eso es difícil de determinar, porque en el fondo es un debate moral», concreta Gurin.

La sentencia del Supremo aporta, además, importantes matices al criterio de prueba. "Se da un toque de atención al empresario. No todo vale", advierte Carlos

González Oliver, presidente de la sección de derecho laboral del ICAB (Ilustre Colegio de Abogados de Barcelona) y explica que hay un matiz novedoso en la sentencia al verificar que las filmaciones en ningún caso pueden usarse para controlar la efectividad del empleado en su puesto de trabajo, las ausencias del mismo o la pérdida de tiempo. "Una cosa es la seguridad y otra muy distinta el control del trabajo", añade. En este sentido, se insiste en que las áreas de descanso del centro de trabajo, zonas de acceso a vestuarios o los servicios no deben estar dotados de cámaras de grabación porque éstas sí vulneran el derecho a la intimidad de los empleados.

Posibles reaperturas

Desde el despacho de abogacía Gispert se corrobora que, tomando como referencia la sentencia del Supremo del pasado 31 de enero, habrá recursos judiciales que estén pendientes de resolución y en los que la prueba de la filmación fue denegada ahora podría solicitarse la reapertura de la causa e insisten en que sienta precedente en la jurisdicción laboral. Isaac González pone en valor este aspecto por cuanto hasta ahora una grabación podía ser prueba incriminatoria en un juzgado de instrucción o en el penal y "era rechazada" en los juzgados sociales.

La judicialización demuestra que las imágenes de las cámaras de seguridad son prueba definitiva, con bastante frecuencia, en hurtos o apropiación indebida enámbitos laborales como, por ejemplo, los casinos -en los que incluso a veces se da la connivencia de empleados y clientes-, supermercados y grandes superficies -adueñándose de productos-, joyerías o negocios mayoristas, entidades financieras... y en hostelería, donde lo que más abunda es la falta de registro de los pedidos.

MÁS DE LA MITAD SON DENUNCIAS LABORALES

Las cifras de 2016 que maneja la Autoridad Catalana de Protección de Datos demuestran que poco más de la mitad (54%) de las denuncias por vulneración de la privacidad con el uso de cámaras de videovigilancia correspondieron a controles realizados en el ámbito laboral. Del total de denuncias recibidas, un 8% se centraban en la utilización de dispositivos de grabación. A nivel estatal, en 2015, este tipo de reclamaciones representaron el 2% del total de consultas recibidas por la Agencia Española de Protección de Datos.

18/04/2017. ¿Qué es una evaluación de impacto en protección de datos? FUENTE: elderecho.com

Iniciada la cuenta atrás para adecuarse al Reglamento Europeo de Protección de Datos.

Hasta que se publicó el Reglamento General de Protección de Datos[1] (RGPD), la normativa europea no hacía mención expresa alguna a las evaluaciones de impacto en protección de datos o a las evaluaciones de impacto de privacidad. El mencionado Reglamento las regula por primera vez y, si bien en otros países existe más conocimiento y desarrollo de esta figura, en España podemos decir que estamos en una etapa algo temprana al respecto.

Sin embargo, tal y como ha indicado la Agencia Española de Protección de Datos (AEPD), conviene aprovechar el tiempo que queda hasta la efectiva aplicación del RGPD, en mayo de 2018, para ir adaptándose a este nuevo marco legal, a fin de que, llegado ese momento, las organizaciones se encuentren en el mayor grado posible de cumplimiento.

Bajo mi punto de vista, junto con la privacidad por defecto y desde el diseño, las evaluaciones de impacto en protección de datos es una de las herramientas que, bien aplicada y sobre todo en aquellos supuestos en que resulte obligatorio realizarlas, contribuye en gran medida a acreditar que la entidad cumple con el principio de responsabilidad proactiva (accountability) que exige el Reglamento.

El principal objetivo de toda EIPD es reducir los riesgos para la protección de los datos personales y para otros derechos que puedan verse afectados como consecuencia del tratamiento de los datos de carácter personal. En consecuencia, el análisis de los riesgos y la medición de éstos, es una parte importante de toda evaluación de impacto. Sin embargo, no es la única y, además, en el caso de las EIPD, el análisis de riesgos debe llevarse a cabo con ciertas particularidades que lo distinguen de otro tipo de análisis de riesgos que puede convenir realizar también en la organización.

A su vez, con una EIPD se pueden obtener otros beneficios o ventajas como, por ejemplo, entender mejor lo que implica la protección de datos, conseguir una gestión más eficaz de los activos y procesos de la entidad, ayuda a la continuidad del negocio y, entre otras cosas, facilita también el cumplimiento de otras muchas obligaciones requeridas por el RGPD.

Ahora bien, las evaluaciones de impacto en protección de datos no son únicamente una herramienta muy útil y conveniente, sino que resultan obligatorias para organizaciones que lleven a cabo determinadas operaciones de tratamiento de datos. Los supuestos que el Reglamento contempla como obligatorios son aquellos en que se produzcan:

a) decisiones automatizadas, que originen efectos jurídicos hacia el interesado (persona a quien corresponden los datos personales) o le afecte significativamente,

b) tratamientos a gran escala de categorías especiales de datos o de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas,

c) observación sistemática a gran escala de una zona de acceso público,

d) operaciones que, a criterio de la autoridad de control competente, impliquen un alto riesgo para los derechos de los interesados y

e) cualquier tratamiento de datos que, por su naturaleza, alcance, contexto o fines, implique un alto riesgo para los derechos y libertades de las personas físicas, y en particular si utiliza nuevas tecnologías.

El RGPD no nos ofrece muchas pistas sobre cómo llevar a cabo estas evaluaciones de impacto, y las guías y metodologías existentes hasta ahora eran pre-reglamento. Por tanto, se hace necesario abordar una metodología que abarque todas las fases necesarias y, dentro de cada una de éstas, los pasos a dar para que, cumpliendo con las exigencias del Reglamento, se pueda, en definitiva y resumen:

Identificar cada uno de los riesgos existentes dentro de cada tipo de riesgos que se puedan clasificar.

Evaluar adecuadamente cada uno de estos riesgos en función de su origen, naturaleza, particularidad y de su probabilidad y gravedad para los derechos y libertades de los interesados.

Conocer las opciones existentes ante cada uno de estos riesgos.

Y finalmente decidir qué medida adoptar al respecto para evitar o mitigar los mismos.

21/04/2017. El "derecho al olvido". FUENTE: computerworld.es.

El "derecho al olvido"

Para que la distancia sea el olvido: El "derecho al olvido", uno de los cambios del nuevo Reglamento de Protección de Datos de la Unión Europea.

El día a día de cualquier persona, y más de las empresas, está lleno de gestión de datos. Desde la aparición de los primeros ordenadores, la evolución de la informática y las TICs hizo que irrumpiese en el mundo el ARPANET, posterior INTERNET, conectó el uso de la telefonía inicialmente, las telecomunicaciones después, con la informática. Este nuevo instrumento de comunicación revolucionó

el tratamiento de los datos, al permitir una transmisión masiva y constante de los mismos, inicialmente de ordenador a ordenador, y después a conjuntos de ordenadores a través de la Red. El uso masivo de la Red, la Internet de la Cosas, el Cloud Computing y la Business Intelligence han multiplicado exponencialmente el impacto sobre el tratamiento de los de datos, al hacer infinito el volumen de los mismos que pueden estar circulando a través de estos sistemas. Desde el punto de vista jurídico, esta revolución en la gestión de los datos ha demandado un cambio en la protección de algunos derechos que se ven afectados, en especial el derecho a la protección de los datos.

En esta línea, una de las últimas reformas que ha llevado a cabo la Unión Europea (UE) ha sido la de la normativa de protección de datos. Cuatro intensos años de trabajo, consultas y discusiones entre los distintos Estados miembros, instituciones comunitarias y particulares, han dado como fruto el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. El Reglamento es una norma compleja, que va a implicar cambios sustanciales en las normativas de los Estados miembros, y en la organización y gestión de las cuestiones de protección de datos de las empresas, incluso en el desarrollo de las actividades de algunas empresas en concreto, como los buscadores de Internet.

Los cambios han venido inspirados principalmente por la irrupción de Internet y los problemas que ha supuesto para la gestión de los datos personales. La Red de redes no tiene fronteras y resulta complicado aplicarle normas territoriales, pero por otra parte, no se puede dejar que la propia Red se autorregule, y que sea ella, o los que la gestionan, quienes decidan que se protege y que no. Ante esta situación, la UE se ha posicionado buscando mecanismos para proteger a sus particulares, y los datos que de los mismo puedan circular por Internet, tanto dentro como fuera de sus fronteras. Un ejemplo de esta toma de posición lo encontramos en el llamado “derecho al olvido” o derecho a la supresión de datos. En esencia, este derecho supone un actualización y adaptación a Internet del derecho a la cancelación de los datos, recogido ya en la Directiva 95/46/CE. En la aplicación de este derecho, se plantean dos problemas: en primer lugar, su propio contenido, puesto que el artículo 17 del Reglamento no define claramente el contenido de este derecho. Y en segundo lugar, la práctica que se le pueda dar.

En cuanto a su contenido, el derecho al olvido implica que, bajo determinadas circunstancias, los particulares pueden solicitar que se borren sus datos de la fuente en la que se contengan. La magnitud que ha adquirido este derecho ha venido dada porque se ha solicitado a los buscadores de internet que ejecuten este derecho, es decir, que procedan al borrado de datos, cuando así lo solicite un particular y resulte coherente proceder al borrado de acuerdo con la normativa (que se retire el consentimiento, que exista desconexión entre el consentimiento y el fin para el que fueron recabados, etc). Los buscadores de internet se han resistido a proceder al borrado, entre otras razones por la dificultad técnica que esto supone, en un sistema de tráfico de datos constante. Sin embargo, la posición de la UE, mantenida por el TJUE en el asunto Google Spain, ha sido la de aplicar este derecho

para proteger los derechos de los particulares, frente a otros posibles intereses en juego.

Por lo que respecta a la aplicación del mismo, resulta curioso que desde el punto de vista jurídico y de acuerdo con las normas sobre competencia judicial internacional y sobre determinación de la ley aplicable del nuevo Reglamento, dentro de la Unión Europea se puede reclamar judicialmente el cumplimiento de este derecho, incluso frente a operadores de Internet situados fuera de las fronteras de la UE, como sería el caso de Google Internacional. No obstante, puede resultar complicado el caso de tener que solicitar la ejecución de una sentencia del Tribunal de Justicia de la Unión Europea (TJUE) por la que se reconoce este derecho en un tercer Estado extracomunitario, en especial si la solicitud de reconocimiento y ejecución se dirige a los Estados Unidos, cuyo concepto de la protección de datos es distinto al reconocido en la UE. La complicación deriva, no sólo porque la UE está siendo pionera en el reconocimiento legal de este derecho, sino también porque afloran a través de él las diferencias en la protección del bien jurídico "privacidad", que es en última instancia lo que trata de proteger el derecho al olvido. En el ejemplo citado, la sentencia del TJUE en el asunto Google Spain reconocía el derecho de los particulares a que Google internacional borrara de sus servidores los datos que los ciudadanos comunitarios les solicitaran. La sede de Google internacional se encuentra en California, por lo que era fácil pensar que los ciudadanos de la UE tendrían que tratar de ejecutar la sentencia europea en territorio americano. Sin embargo, la realidad ha hecho que la empresa americana se aviniera a cumplir con la sentencia, sin necesidad de instar un cumplimiento forzoso. Eso sí el cumplimiento de esta sentencia, y del ejercicio del derecho al olvido ha supuesto que la empresa se ha visto obligada a crear todo un mecanismo (y probablemente un departamento) que gestione las solicitudes de borrado de datos en el ejercicio del derecho al olvido.

Este ejemplo del derecho al olvido es solo uno de los supuestos en los que las empresas se van a ver obligadas a cambiar su gestión de los datos para poder cumplir con la nueva normativa de protección de datos. La forma de almacenar y supervisar si se cumple con las obligaciones de protección de datos, la manera de recabar el consentimiento, o las normas sobre portabilidad de datos son otras de las novedades que van a afectar a algunas de las prácticas de las empresas comunitarias.

04/05/2017. Tus datos se venden por 7 céntimos de euro. FUENTE: elpais.com

Tus datos se venden por 7 céntimos de euro

Un informe de Amnistía Internacional revela la venta de información de 1,8 millones de musulmanes por 126.851 euros. Este comercio se expande gracias al 'big data'

¿Cuántas veces al año marca usted una casilla en la que autoriza al acceso y cesión de sus datos? ¿Cinco, diez? Haga bien la cuenta. Aunque la espada de Damocles apunte a las redes sociales, en realidad, los datos se ceden en cualquier

transacción. Al contratar una tarjeta de crédito, hacer una compra, dar de alta una wifi, participar en una encuesta, al visitar páginas web… Datos que individualmente no tienen valor, juntos constituyen una nueva minería, más valiosa que la del oro. No son solo los datos privados de cada persona, sino los de cada actividad individual, cada compra o cada emoticono con el que se reacciona a los comentarios en las redes sociales, el big data permite obtener las preferencias políticas, religiosas, sexuales y alimenticias, así como la situación económica, sanitaria, policial e incluso emocional de cada persona. Los algoritmos secretos que usan estas empresas son cada vez más sofisticados y, por tanto, las posibilidades, infinitas.

Un equipo de investigadores de Amnistía Internacional (AI) revela la oferta por parte de una de estas empresas, Exact Data, de los datos de 1,8 millones de musulmanes por 138.380 dólares (126.851 euros), es decir, a razón de 7,5 centavos (7 céntimos de euro) por persona. La compañía en cuestión, "presume de tener una base de datos total de 200 millones de contactos de Estados Unidos que se pueden filtrar mediante 450 categorías, tales como religión y etnia", detalla el informe y ha podido comprobar este periódico en la propia web. Este sitio, ExactData.com, también ofrece "un abanico de listas de contactos preconfiguradas", por ejemplo, las de "estadounidenses hispanos no asimilados" (en referencia a los que no están integrados en la sociedad de EE UU, independientemente de su condición legal)".

En Europa hay alrededor de 50 grandes empresas 'data brokers'; en el mundo, nadie lo sabe

Muchas de las empresas que viven de la venta de datos privados de personas no se esconden en Internet.

"El hecho de que se pueda comerciar con estas listas y puedan acabar en manos indebidas, hace posible que se utilicen para iniciativas que podrían vulnerar los derechos humanos, como la creación de sofisticados perfiles que pueden atentan contra la privacidad", advierte el director de Comunicación de AI España, Miguel Ángel Calderón.

Justo dentro de un año, en mayo de 2018, empezará a aplicarse un nuevo reglamento europeo de protección de datos más estricto que el actual, que se espera mejore el control de los ciudadanos sobre los datos personales que ceden a terceros, resalta Calderón.

Una de las autoras de esta investigación, asesora de Tecnología y Derechos Humanos de esta organización, Tanya O'Carroll, explica desde Londres que el comercio con datos privados "es un negocio floreciente". "El inmenso avance experimentado por el big data en la última década ha permitido que los data brokers [empresas de comercio de datos] lo sepan todo de ti", afirma esta experta. "Los datos pequeños y abstractos, que no tienen ninguna importancia por sí solos, cruzados, por ejemplo, con los me gusta de Facebook, cobran gran valor".

O'Carroll resalta uno de los aspectos más relevantes de esta situación: el anonimato de esta industria. "No es transparente. Saben mucho de ti, pero tú no

sabes ni quién tiene tus datos ni el nombre de estas empresas". Solo en Europa, operan al menos 50 empresas de data brokers, según la lista recopilada por Amnistía Internacional. ¿Y en el resto del mundo? "Es imposible saber las que hay en Estados Unidos o en Asia. Cientos", responde O'Carroll. ¿Qué puede hacer entonces cada usuario por protegerse de este comercio o, al menos, por tener algún control sobre sus datos?

UNAS CONFUSAS POLÍTICAS DE PRIVACIDAD

La globalización de Internet, con todas sus bondades, complica muchísimo la tutela de nuestros datos. España tiene fama de ser uno de los países más proteccionistas. Dos leyes, la General de Telecomunicaciones y la de Servicios de la Sociedad de la Información, velan por ello, como recuerda Jesús Rubí, adjunto a la directora de la Agencia Española de Protección de Datos. "El nuevo reglamento europeo, que se aplicará en 2018, supone un gran avance. Prevé que, en los casos de que la compañía no tenga un establecimiento en la UE, cuando los servicios son para usuarios europeos o se monitoriza su conducta, la empresa tiene que cumplir la normativa europea de protección de datos y tiene que asignar un representante. Es un paso muy importante".

Sobre el consentimiento de ceder los datos por parte de los usuarios, Rubí explica que "la situación legal ha ido evolucionando hasta tener que detallarse las finalidades específicas que se van a dar a esos datos. Y debe ser libre, y no denegarse de manera injustificada la prestación del servicio para obtenerlo". "El principal problema", concluye Rubí, "es que las políticas de privacidad siguen siendo confusas y poco accesibles, porque, en muchos casos, las empresas ofrecen servicios muy diversos".

Privacidad y seguridad

"La gente se ha acostumbrado a ceder sus datos para cualquier cosa sin pensar que es inseguro y que valen dinero", contesta Álvaro Ortigosa, director del Centro Nacional de Excelencia en Ciberseguridad (CNEC)de la Universidad Autónoma de Madrid. "Pero, además, aparte de pensar en la privacidad, deberíamos pensar también en la seguridad, en la vulnerabilidad de esas bases de datos, que son muy jugosas", advierte Ortigosa.

Este experto cree que los usuarios deben apuntar las direcciones de todas las webs a las que han cedido sus datos puntualmente "y escribir luego para que los borren. Por sistema". En cuanto a los datos vinculados a un servicio, como la red wifi de la vivienda habitual, Ortigosa considera que la legislación debería obligar a las empresas a limpiar todos los datos de particulares cada ciertos meses de forma sistemática.

Pero, ¿cómo trabajan estas empresas? Borja González del Regueral, vicedecano de IE School of Human Science & Technology, explica que "es un negocio en el que o bien se venden directamente los datos o bien se ceden, aunque con la nueva directiva europea, estas empresas están obligadas, entre otras cosas, a informar al usuario de la cesión de los datos a terceras partes". El principal problema, apunta este especialista del Instituto de Empresa, "es que es tu responsabilidad leerte el

contrato cuando cedes tus datos pero ¿quién se lee 15 páginas cada vez que se compra unos pantalones por Internet?". "Por eso, se debe aumentar la transparencia", opina González del Regueral.

Pero los data brokers no solo obtienen información de las transacciones o de las redes sociales. "Agregan numerosos datos de muchos sitios", prosigue este experto. "De los registros públicos o de cualquier actividad que esté en documentos que haya volcado en Internet algún organismo". Y tampoco son los únicos que comercian con nuestra información privada. "Los datos son un activo para cualquier empresa. La cuestión es saber cuál es la manera más ética de comerciar con ellos".

Y ahora, vuelva a hacer la cuenta. ¿Cuántas veces ha cedido sus datos en el último año? ¿50? "Hay una tendencia al alza en incorporar este negocio en las empresas tradicionales", remacha González del Regueral.

05/05/2017. El contrato para el tratamiento de datos debe incluir certificados de seguridad. FUENTE; eleconomista.es

El contrato para el tratamiento de datos debe incluir certificados de seguridad

El responsable del tratamiento exigirá al encargado que pruebe sus garantías

La transferencia fuera de la UE no podrá rebajar el nivel de protección

La empresa que contrate o encargue a otra el tratamiento de datos deberá asegurarse de que ésta tiene las medidas técnicas y organizativas adecuadas para garantizar los niveles de seguridad y la protección de los derechos exigidos por el Reglamento General de Protección de Datos (RGPD). Unas garantías que podrán demostrarse a través de certificados de protección de datos o la adhesión a códigos de conducta.

Así lo determinan las Directrices del Grupo de Trabajo del Artículo 29 -foro que integra a las autoridades nacionales y europeas de privacidad- que ofrecen las pautas sobre el contenido y la forma que debe tener el contrato entre el responsable del tratamiento -la empresa u organización contratante- y el encargado del mismo -la empresa contratada-.

El documento, difundido por la Agencia Española de Protección de Datos (AEPD), se encuadra dentro de los materiales que se están poniendo a disposición de las

empresas de cara a la entrada en vigor del RGPD en mayo de 2018, y que supone una revolución en la concepción de la privacidad.

De acuerdo con el mismo, el responsable del tratamiento debe exigir al encargado "garantías suficientes" en relación a "conocimientos especializados, fiabilidad y recursos" que le permitan cumplir con todos los requisitos del procesamiento de datos, especialmente las medidas de seguridad.

La relación entre el responsable y el encargado deberá formalizarse a través de un contrato o un acto jurídico similar que, en todo caso, debe constar por escrito y en formato electrónico.

Una de las novedades que introduce el RGPD es que dicha relación también puede regularse a través de un acto jurídico unilateral del responsable del tratamiento, como es el caso de una resolución administrativa.

Informar a los interesados

A pesar de que la normativa no impone al responsable el deber de informar a los interesados de la contratación de un encargo del tratamiento, las Directrices sí recomiendan que en determinadas circunstancias -por ejemplo, en función de la naturaleza del tratamiento o de los datos tratados- sí se produzca tal comunicación "para una mayor transparencia".

El encargo del tratamiento, en cualquier caso, no traspasa la responsabilidad del correcto procesamiento de datos y del respeto a los derechos de los interesados. Según especifica el documento, el responsable no pierde esa consideración en ningún caso.

Asimismo, el contrato no podrá emplearse como un mecanismo para rebajar las exigencias y los estándares de seguridad que impone el Reglamento por la vía de contratar un encargado de un país fuera de la UE. El texto precisa que en estos contratos deberán mantenerse los niveles de protección que garantiza la norma.

11/05/2017. La AEPD publica un 'Código de buenas prácticas en protección de datos para proyectos de Big Data'. FUENTE: Noticias.juridicas.com

La AEPD publica un 'Código de buenas prácticas en protección de datos para proyectos de Big Data'

La Agencia Española de Protección de Datos (AEPD) e ISMS Forum Spain han editado conjuntamente un código de buenas prácticas en colaboración con empresas y profesionales independientes, orientado a asesorar en materia de protección de datos a todas aquellas entidades que se estén planteando poner en marcha proyectos de Big Data. El documento toma como referencia el nuevo Reglamento Europeo de Protección de Datos, que será aplicable el 25 de mayo de 2018.

El Código de buenas prácticas en protección de datos para proyectos de Big Data se presenta en el marco de la XIX Jornada Internacional de la Seguridad de la

¿Qué es el Código de buenas prácticas en protección de datos para proyectos de Big Data?

El Código de buenas prácticas en protección de datos para proyectos de Big Data de la AEPD e ISMS Forum Spain constituye un punto de partida de referencia práctica para las empresas, con un primer bloque que incluye el régimen jurídico aplicable y cuestiones clave como la definición del responsable del tratamiento de los datos y el encargado. También se analizan las principales implicaciones derivadas de los tratamientos basados estas técnicas, como el origen, calidad y conservación de los datos; la procedencia de los mismos; la trasparencia que se debe ofrecer en la información previa facilitada a los afectados; la obtención del consentimiento de estos o, en su caso, el interés legítimo para tratar esos datos; los usos no previstos en el momento inicial, y el ejercicio de derechos por parte de los ciudadanos cuya información se está tratando.

Generación de perfiles de consumidores o profiling

Las iniciativas basadas en Big Data pueden aportar beneficios sociales en sectores clave y nuevas posibilidades de negocio a las organizaciones a partir del análisis de grandes cantidades de datos a los que se aplican algoritmos con el fin de establecer correlaciones o elaborar patrones. Sin embargo, también surgen dudas y preocupaciones sobre usos que pueden no ser lícitos por realizarse sin respaldo legal o por generar abusos, como la modificación de precios de un producto en función de lo que esté dispuesto a pagar un usuario al que previamente se ha analizado.

En este sentido, la generación de perfiles de consumidores o profiling es sin duda uno de los usos principales del Big Data, y puede entrañar riesgos por posibles tratamientos basados en predicciones si se utilizan de forma discriminatoria excluyendo a sectores minoritarios apoyándose en los datos analizados. Teniendo en cuenta estos aspectos, el desarrollo y la puesta en marcha de proyectos de Big Data implica una importante responsabilidad para aquellas entidades que los implementan, que deben preservar la privacidad de las personas adoptando acciones y soluciones de tipo jurídico, organizativo y técnico.

Privacidad desde el diseño

Un segundo bloque examina los aspectos que deben tener en cuenta las entidades que van a utilizar Big Data para garantizar la protección de datos y la privacidad de los ciudadanos, destacando principios como la privacidad desde el diseño o la responsabilidad de las entidades a la hora de establecer mecanismos de garantía y cumplimiento de las obligaciones de protección de datos (accountability). Igualmente, el documento detalla, entre otros aspectos, la necesidad de realizar evaluaciones de impacto en proyectos de este tipo para minimizar los riesgos o la posibilidad de optar por la anonimización irreversible de los datos. El Código finaliza con una revisión de las medidas tecnológicas imprescindibles en materia de privacidad y seguridad para crear un entorno adecuado de confianza para el desarrollo de tecnologías Big Data.

17/05/2017. Multan a Facebook por no cumplir la Ley de Protección de Datos. FUENTE: cincodias.es

Desde luego se trata de un tema controvertido el de las redes sociales y la privacidad de los usuarios, ya que para estos últimos no está demasiado clara la línea de hasta dónde están protegidos sus derechos para con la redes sociales y estas a su vez se aprovechan de ello para poder acceder a mayor y mejor información sobre todos sus usuarios. Y prueba de ello es que ahora hemos conocido que la red social Facebook ha sido multada con 150.000 euros por incumplir la ley de protección de datos. Algo que podría ser sólo el principio, ya que varios países europeos están ya alerta de estas prácticas de Facebook.

Facebook sigue incumpliendo la Ley de Protección de Datos

El CNIL, un organismo oficial francés que vela por los derechos y la protección de datos de los ciudadanos de aquel país, ha multado a Facebook con 150.000 euros al estimar tras una exhaustiva investigación que la red social no está respetando los derechos de los ciudadanos en el uso de la red social respecto de la privacidad de sus datos, violando la Ley de Protección de Datos del país vecino. Un móvil con la red social Facebook, que ha sido multada

Aunque esta sanción llegue ahora, en realidad responde a un cambio en la política de privacidad de la red social introducida en el año 2015. En el trasfondo de estas prácticas de Facebook se encuentran los datos de los usuarios de la red social que son compartidos con terceros, como anunciantes, sin el conocimiento explícito de los consumidores y usuarios de la red social. Pero esta investigación se ha estado llevando a cabo en varios países, entre ellos España, y todo apunta a que podrían llegar nuevas multas para Facebook por su comportamiento similar con la Ley de Protección de Datos con los usuarios de otros países.

Facebook ha hecho caso omiso a las advertencias.

Esta multa sólo es una muestra más de la tortuosa relación de Facebook con las autoridades de los distintos gobiernos europeos. De hecho en enero de 2016 el CNIL francés ya advirtió a Facebook de que tenía tres meses para rectificar su actitud en este caso. Pero a pesar de las advertencias la red social ha seguido incumpliendo sistemáticamente la Ley, no informando a los usuarios sobre los derechos y uso de la red social, así como la falta de consentimiento por parte de los usuarios a la distribución de algunos datos sensibles de su perfil. En total Facebook ha violado sistemáticamente seis de los apartados de la Ley de Protección de datos, razón por la cual Facebook .Inc y Facebook Ireland han sido multadas con 150.000 euros.

25/05/2017. La AEPD publica una guía práctica para difundir el derecho a la protección de datos entre los ciudadanos. FUENTE: agpd.es

La AEPD publica una guía práctica para difundir el derecho a la protección de datos entre los ciudadanos.

'Protección de Datos: Guía para el Ciudadano' recoge numerosas referencias a los cambios que incorpora el nuevo Reglamento General, que será aplicable el 25 de mayo de 2018, e incluye las principales novedades respecto al ejercicio de derechos.

Repasa los tradicionales derechos ARCO e incluye otros como el derecho al olvido, el nuevo derecho a la portabilidad, o la forma de solicitar la eliminación de fotos y vídeos en internet y qué hacer en caso de no recibir respuesta

Contiene ejemplos de los tratamientos de datos que más afectan a los ciudadanos, como ocurre en el caso de las comunidades de vecinos, los llamados ficheros de morosos, la videovigilancia o la publicidad, entre otros

(Madrid, 25 de mayo de 2017). La Agencia Española de Protección de Datos (AEPD) ha presentado 'Protección de Datos: Guía para el Ciudadano' en el marco de la 9ª Sesión Anual de la AEPD, un documento que recoge de forma práctica las claves necesarias para que los ciudadanos conozcan qué derechos les amparan y cómo ejercerlos, y qué obligaciones deben cumplir aquellos que traten sus datos personales. Los datos que maneja la Agencia respecto a las consultas recibidas constatan la importancia que los ciudadanos conceden a la protección de sus datos personales y a su privacidad. Así, en 2016 la AEPD recibió cerca de 237.000 consultas, casi un 9% más que en 2015. Por su parte, el Barómetro del CIS de febrero de 2017 también destacó esa importancia al señalar que al 76% de los españoles les preocupa la protección de datos personales y el posible uso de su información personal por terceros.

El Reglamento General de Protección de Datos (RGPD), que comenzará a aplicarse el 25 de mayo de 2018, implica cambios respecto a la normativa actual. Por ello, la Guía para el ciudadano contiene numerosas referencias a la nueva normativa, incluyendo las principales novedades respecto al ejercicio de derechos, detallando qué se puede solicitar en cada uno de los casos.

La Guía repasa los tradicionales derechos de acceso, rectificación, cancelación y oposición (derechos ARCO), la forma de ejercerlos y los plazos legales en los que el ciudadano debe obtenerse una respuesta, incluyendo también aspectos relacionados con el nuevo derecho a la portabilidad, en qué consiste y cómo ejercer el derecho al olvido, o cómo solicitar la eliminación de fotos y vídeos de internet.

Asimismo, la Guía contiene ejemplos de los tratamientos de datos que más repercusión pueden tener en los ciudadanos, como ocurre con los llamados ficheros de morosos, describiendo los requisitos que deben cumplirse para que los datos de una persona puedan ser incluidos en uno de estos ficheros. En este sentido, la inclusión indebida en ficheros de morosidad produce unos efectos especialmente negativos para los afectados, por lo que es imprescindible que las empresas extremen su diligencia antes de comunicar una información inexacta. Por otro lado, el documento recoge otros ámbitos concretos en los que se efectúan tratamientos de datos, como las comunidades de vecinos, la videovigilancia o la publicidad.

‘Protección de Datos: Guía para el Ciudadano’ ofrece ejemplos de casos concretos y enlaces con información adicional disponible en la web de la Agencia para que el

ciudadano pueda profundizar sobre las garantías de su derecho a la protección de datos. Además, contempla un glosario con los términos y definiciones utilizadas, así como un listado de recursos online para facilitar el ejercicio de derechos, incluyendo la posibilidad de interponer una denuncia o solicitar una tutela de derechos.

La AEPD sigue trabajando en su objetivo de difundir entre la ciudadanía una cultura de protección de datos, para lo cual viene desarrollando diferentes acciones e iniciativas específicas entre las que se encuentran la Guía sobre Privacidad y Seguridad de internet o la renovación de las consultas más frecuentes planteadas ante la Agencia (FAQs).

31/05/2017. UE prohíbe a empresas el uso de datos biométricos sin consentimiento previo. FUENTE: lavanguardia.com

UE prohíbe a empresas el uso de datos biométricos sin consentimiento previo

Barcelona, 31 may (EFE).- La entrada en vigor del Reglamento General de Protección de Datos (RGPD) de la Unión Europea prohíbe a las empresas utilizar datos biométricos, como las huellas o el reconocimiento facial, sin un consentimiento previo de los usuarios.

Según la Autoridad Catalana de Protección de Datos (ACPD), con el nuevo reglamento muchos gimnasios o aplicaciones para móviles que utilizan este tipo de identificación quedan obligados a hacer una evaluación de la protección y el tratamiento que dan a estos datos y, en su caso, a aplicar las medidas de seguridad técnicas y organizativas adecuadas.

La normativa entiende por tratamiento "cualquier operación sobre los datos personales que de manera automatizada, o no, implique la recogida, el registro, la organización o utilización, entre otros, de estos datos personales".

A partir de ahora, las imágenes faciales, las huellas, la identificación por voz y el escáner del iris o de retina deberán ser tratadas de manera "lícita, leal y transparente", y solo podrán recogerse "con fines determinados, explícitos y legítimos".

El reglamento recoge que las empresas que no se adecúen a la normativa europea podrán recibir sanciones que pueden alcanzar los 20 millones de euros o el 4% del volumen de negocio anual.

La directora de la Autoridad Catalana de Protección de Datos, Maria Àngels Barbarà, ha recordado que "el análisis de proporcionalidad entre los datos recogidos, las tecnologías utilizadas para hacerlo y la finalidad perseguida forma parte de la rendición de cuentas que debe regir todas las decisiones que toma el responsable de su tratamiento".

También la banca 'online' o las plataformas que ofrezcan un servicio de pago a través de datos como la huella digital deberán contar con las medidas de protección necesarias.

La APDCAT propone la pseudonimización como una de las posibilidades para proteger los derechos de los usuarios, ya que permite el tratamiento de datos personales de forma que no se pueden atribuir a un individuo concreto sin una información adicional. EFE

01/06/2017. Crónica sobre la 9ª Sesión Anual Abierta de la AEPD. FUENTE: periodistadigital.com

Crónica sobre la 9ª Sesión Anual Abierta de la AEPD.

La jornada estuvo marcada por el Reglamento General de Protección de Datos

El pasado 25 de mayo se celebró la 9ª Sesión Abierta de la Agencia Española de Protección de Datos (AEPD), a la que Áudea Seguridad de la Información asistió. Estos son los temas más destacables que se mencionaron acerca del Reglamento General de Protección de Datos (GDPR).

Nueva herramienta

La Agencia, además de las Guías u orientaciones que han publicado para los responsables y encargados del tratamiento, anunció la próxima implantación de una herramienta dirigida a las Pymes y micropymes que les servirá de apoyo para cumplir con el GDPR. Va dirigida a las empresas y profesionales que realicen un tratamiento de datos de bajo riesgo y la herramienta propondrá los documentos mínimos necesarios para cumplir con el GDPR, como pueden ser el registro de actividades de tratamiento, cláusulas informativas o las medidas de seguridad que, como mínimo, deben cumplir.

Novedad

En la Sesión también se trataron algunas de las novedades que el GDPR añade respecto del texto de la LOPD, como por ejemplo:

La necesidad de justificar la base jurídica sobre la que se legitima el tratamiento (sea el consentimiento u otra de las bases previstas en el GDPR).

La obligación de establecer un plazo de conservación de los datos desde el momento de la recogida.

La anulación de los consentimientos tácitos recabados durante estos años.

La necesidad de volver a firmar contratos de encargo de tratamiento con todos los proveedores que manejen datos personales.

El derecho de portabilidad, que implica la posibilidad de descarga y transmisión a otro prestador de servicios de los datos del interesado, que no deberá afectar al derecho a la intimidad de terceros, salvo circunstancias excepcionales.

En cuanto a las Evaluaciones de Impacto se destacó su importancia para que se cumpla con el principio de Accountability, y la necesidad de que se haga con antelación al tratamiento, para poder detectar y corregir deficiencias (y, en su caso, plantear la oportuna consulta previa a la AEPD).

En lo referente a la seguridad de los datos, no se va a publicar ningún catálogo de medidas de seguridad y todas las medidas implantadas en las empresas deberán estar orientadas al riesgo. Se valoraron distintas opciones de catálogos de medidas que pueden ser utilizadas como referencia, como por ejemplo, los controles del estándar ISO 27002, o los del Esquema Nacional de Seguridad (aprobado por Real Decreto 3/2010).

Certificación para DPO´s

Por otro lado, la Agencia anunció que está trabajando con la Entidad Nacional de Acreditación (ENAC) en la implantación de un esquema de certificación de profesionales que vayan a acceder al puesto de Delegado de Protección de Datos. La intención no es que dicha certificación sea obligatoria, sino que garantice a la empresa la cualificación y capacidad profesional del candidato.

Otras novedades

Por destacar algo positivo, la AEPD resaltó que el apercibimiento, figura que implica la resolución de una infracción sin sanción económica y que hasta ahora tenía un carácter excepcional en la LOPD, ya no tiene tal carácter excepcional en el GDPR. Sin embargo, su aplicación seguirá siendo discrecional para la AEPD, por lo que está por ver si se nota este cambio positivo en la normativa.

Os adelantamos que la AEPD no tiene muchas esperanzas de que la nueva LOPD esté lista antes de mayo de 2018, por lo que parece necesario, mientras tanto, empezar a trabajar ya en la adecuación al GDPR.

Para más información, la AEPD ha puesto a disposición en su web el programa con cada una de las presentaciones de la 9ª Sesión.

13/07/2017. La AEPD presenta su esquema de certificación de delegados de protección de datos. FUENTE; cincodias.elpais.com

La AEPD presenta su esquema de certificación de delegados de protección de datos

La Agencia Española de Protección de Datos ha contado con la colaboración de la Entidad Nacional de Acreditación en la elaboración de este marco de referencia para esta figura

La designación de estos delegados para determinadas entidades es una de las imposiciones del reglamento europeo de protección de datos

La Agencia Española de Protección de Datos (AEPD), en colaboración con la Entidad Nacional de Acreditación (ENAC), ha presentado hoy su Esquema de certificación de Delegados de Protección de Datos. Su elaboración ha contado con la participación de un comité técnico de expertos formado por 23 miembros, entre los que se encuentran representantes de sectores y asociaciones profesionales, empresariales, universidades y Administraciones Públicas. La AEPD se convierte así en la primera Autoridad europea que realiza un Esquema de certificación de delegados de protección de datos.

La AEPD ha optado por promover un sistema de certificación de estos delegados con el objetivo de ofrecer seguridad y fiabilidad tanto a los profesionales de la privacidad como a las empresas y entidades que van a incorporar esta figura a sus organizaciones, ofreciendo un mecanismo que permite certificar que reúnen la cualificación profesional y los conocimientos requeridos. Las certificaciones serán otorgadas por entidades certificadoras debidamente acreditadas por ENAC, siguiendo criterios de acreditación y certificación elaborados por la AEPD en colaboración con los sectores afectados.

La certificación no es la única vía para ser delegado de protección de datos y en ningún caso será obligatorio utilizar un determinado esquema, si bien la Agencia ha considerado necesario ofrecer un punto de referencia al mercado sobre los contenidos y elementos de un mecanismo de certificación que pueda servir como garantía para acreditar la cualificación y capacidad profesional de los candidatos a Delegado de Protección de Datos.

La directora de la AEPD, Mar España, ha destacado durante la presentación que "promover un sistema de certificación de delegados de protección de datos es una herramienta útil a la hora de evaluar que los candidatos a ocupar estos puestos reúnen las cualificaciones profesionales y los conocimientos requeridos". Además ha querido inisistir en "la gran importancia de los profesionales de la privacidad como elemento clave para el desarrollo de una economía digital innovadora y a la vez respetuosa con los derechos de los ciudadanos". Por su parte, la directora general de ENAC, Beatriz Rivera, ha señalado que "la certificación acreditada aportará a las organizaciones que requieran los servicios de un delegado de protección de datos una información fiable, transparente y simétrica sobre los profesionales, permitiéndoles así una elección informada y basada en competencias".

El Esquema de certificación de Delegados de Protección de Datos de la Agencia se estructura en tres partes: la AEPD como propietaria y responsable del esquema, ENAC como encargada de los requisitos que deben cumplir los certificadores y, finalmente, las propias entidades de certificación.

La creación de este Esquema de certificación de Delegados de Protección de Datos de la AEPD es el punto de partida en un proceso de mejora continua y revisión constante que será necesario realimentar tras su puesta en marcha con la experiencia práctica del acreditador y certificador. A este respecto, la Agencia y ENAC han suscrito un convenio de colaboración para coordinar sus actuaciones en el marco de sus respectivas actividades y competencias.

19/07/2017. Los centros sanitarios se preparan para contratar DPOs. FUENTE: redaccionmedica.com

Los centros sanitarios se preparan para contratar DPOs

Los hospitales y centros de salud se preparan ya para una de las consecuencias de mayor impacto del Reglamento General de Protección de Datos (RGPD): la obligatoriedad de contar con un delegado de Protección de Datos (DPO) en cada uno de ellos a partir del 25 de mayo de 2018. Esto se traducirá, previsiblemente, en una contratación masiva de profesionales especializados en la protección de

datos en los próximos meses.

¿Por qué es obligatorio para hospitales y centros de salud contar con un Delegado de Protección de Datos?

El RGPD estipula, en su artículo 37, que el encargado del tratamiento, en este caso el centro sanitario, deberá designar un delegado de protección de datos. La razón de esta obligatoriedad es el hecho de que los datos relativos a la salud entran dentro de las categorías especiales de datos y la ley estipula que todos aquellos encargados de tratamiento cuyas actividades "consistan en el tratamiento a gran escala de categorías especiales de datos personales" deben disponer de un DPO.

Teniendo en cuenta que el número de centros sanitarios en España está cerca de los 4.000, las tipologías de profesionales con las cualificaciones necesarias para desempeñar este puesto estarán en alta demanda en un futuro próximo. El RGPD, ya en vigor, comenzará a aplicarse el 25 de mayo de 2018. Pero ¿qué tipo de profesionales pueden optar al puesto de delegado de Protección de Datos?

A este respecto, la ley dice: "El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39."

No existe, por tanto, una obligatoriedad de certificación específica alguna, si bien sí puede ser útil para dotar de garantías a las empresas a la hora de contratar a un profesional, aumentando las posibilidades de que sea alguien con capacidad para llevar a cabo las tareas requeridas para el puesto.

La propia Agencia Española de Protección de Datos, comentando la certificación que ya prepara, aclaró que "si bien esta certificación como DPO es totalmente voluntaria y, por tanto, para su ejercicio no es necesario poseer la misma, el hecho de obtenerla supone una garantía tanto de la competencia profesional certificada como del ejercicio de la mencionada competencia".

También es necesario subrayar dos aspectos fundamentales. Uno, que el papel del delegado de Protección de Datos puede ser desempeñado por un proveedor externo ("El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios") y dos, que una misma persona prestar sus servicios a más de una organización dentro de un mismo grupo ("Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento").

24/07/2017. Protección de Datos promete flexibilidad en las multas a los abogados. FUENTE: eleconomista.es

Protección de Datos promete flexibilidad en las multas a los abogados.

La Agencia "como regla general" evitará las sanciones a los despachos.

Consejos y colegios pueden contratar un DPO y ofrecerlo a los profesionales.

Mensaje de tranquilidad de la Agencia Española de Protección de Datos (AEPD) a la abogacía, un sector que tendrá que realizar un importante esfuerzo de adaptación a la nueva normativa de privacidad y, además, del que surgirán muchos de los profesionales que se ocuparán de la materia tanto en el seno de las empresas como asesorando de forma externa a las mismas.

"Si nos llega una denuncia contra un abogado y no tiene sanción previa, como regla general, salvo que la conducta sea muy grave, nos acogeremos al mecanismo de apercibimiento. Actuamos con sentido común y flexibilidad", manifestó Mar España, directora de la AEPD, las jornadas sobre la incidencia del el Reglamento General de Protección (RGPD) en la profesión, organizadas por el Consejo General de la Abogacía Española (CGAE).

España también recordó que de acuerdo con la norma europea los abogados no están obligados a hacer evaluaciones de impacto. Para ellos, y para otros autónomos y pymes que realicen tratamientos de bajo riesgo, la AEPD ha diseñado una herramienta que será presentada en septiembre a través de la cual los profesionales podrán obtener toda la documentación que les permite acreditar que cumplen las exigencias del RGPD.

Para asistir a los letrados, además, se publicará antes de final de año un documento específico con orientaciones específicas sobre el análisis de riesgo.

El papel de los colegios

Otro de los mensajes en los que incidió la directora de la Agencia es en la relevancia de los colegios profesionales. Así, el organismo quiere canalizar a través de ellos las consultas que realicen los abogados, de manera que se constituyan en un "primer filtro".

También manifestó que una de las apuestas de Protección de Datos es que los Consejos o los colegios contraten a un delegado de protección de datos –DPO, por sus siglas en inglés– "y se lo ofrezcan a sus profesionales".

No obstante, España incidió en su recomendación que se contrate a DPO certificados, puesto que contarán con unos conocimientos y unas habilidades acreditadas.

Finalmente, la directora de la Agencia también se comprometió a actuar con "sensatez" en el caso de que un despacho sufra una brecha de seguridad. "Habrá miedo a comunicarlas por temor una sanción, pero salvo que haya una negligencia tremenda, trabajaremos con sentido común", explicó.

Precisamente en la seguridad incidió Cecilia Álvarez, presidenta de la Asociación Profesional Española de la Privacidad (APEP)."Los despachos son un target para los ciberataques porque tienen datos muy interesantes", advirtió.

Por su parte, Javier Aparicio, of counsel de Finreg, mostró sus dudas en relación a la posición del letrado con algunos de los datos contenidos en la documentación de un asunto. "No encaja ni con la definición de responsable del tratamiento ni con la

de encargado. A mi entender el abogado está fuera de los dos conceptos y va a plantear muchos roces y fricciones", aseveró.

21/08/2017. Internet, protección de la intimidad y derecho al olvido. FUENTE; vieu.es

Internet, protección de la intimidad y derecho al olvido

La globalización socioeconómica y cultural, acaecida tras el hundimiento de la URSS a principios de la década de 1990, se ha visto impulsada por una verdadera revolución tecnológica mediante el desarrollo exponencial de las TIC's, articuladoras de lo que conocemos como sociedad de la información y el conocimiento. Dentro de este proceso de transformación civilizatoria en marcha, lleno de multitud de dimensiones a analizar desde la perspectiva de la salvaguarda de los derechos humanos, nos interesa destacar la irrupción creciente de los medios de comunicación digital y de las redes sociales en el espacio de intimidad propio de la vida privada de la persona. Una regla básica de sentido común aparece, de inicio, como punto de arranque de esta temática: si nosotros revelamos públicamente lo que pertenece a nuestra vida íntima, familiar o sentimental, nos exponemos a graves consecuencias e, incluso, a la pérdida del derecho a ser protegidos jurídicamente.

Si dejamos de lado la desigualdad social por países o clases sociales en el acceso a Internet –problema de gran relevancia en cuanto a la garantía de unas oportunidades similares de acceso a la información y la cultura para toda la humanidad–, la interconexión en tiempo real que permite la red de comunicación de Internet afecta de lleno a la protección de ciertos derechos civiles ya clásicos en nuestras democracias de inspiración liberal, a saber: el derecho a la intimidad personal y familiar en la vida privada, el derecho al honor (opinión que tiene el individuo de sí mismo adquirida sobre méritos propios) y a la reputación (reconocimiento social de esos méritos propios), así como el derecho a la voz y a la imagen de cada uno. Como fija el art. 12 de la Declaración Universal de Derechos Humanos de 1948, toda persona tiene derecho a la protección de la ley contra cualquier injerencia o ataque a este ámbito de privacidad. Así, teniendo en cuenta el desarrollo normativo de multitud de constituciones democráticas estatales que reconocen la limitación legítima de estas libertades individuales surgida del derecho a una información veraz y públicamente relevante por parte de los mass media, la protección de este ámbito de privacidad personal incluye también un derecho a la rectificación proporcional, gratuita e inmediata por parte de aquel medio de comunicación que haya difundido tanto informaciones falsas o maliciosamente sesgadas como difamaciones o agravios insultantes.

Ahora bien, todo este sistema jurídico de reconocimiento y garantía de derechos fundamentales que, tan razonablemente bien funciona en lo referido a los medios de comunicación tradicionales (prensa, radio, televisión…), encuentra, por desgracia, graves impedimentos para su aplicación efectiva en los nuevos más media digitales. Estos, inevitablemente, plantean novedosas amenazas cuando no habituales vulneraciones de este tipo de derechos protectores de la privacidad del individuo. Tanto es así que la legislación vigente en los diferentes Estados que

componen la sociedad internacional, aun a pesar de las constantes adaptaciones jurídicas llevadas a cabo por el Derecho sobre las TIC's, todavía no ha conseguido articular un sistema de garantías jurídicas bien trabado y efectivo para contrarrestar semejantes vulnerabilidades de los derechos de sus ciudadanos en su integridad. Y ello, en gran medida, en lo que se refiere a Internet, por el espacio universal, casi ubicuo, que ocupa la propia red digital, que, a diferencia otros medios de comunicación de masas, supera de largo el control jurídico practicable por un Estado en el marco reducido de sus fronteras.

Estamos, pues, ante un gran reto para el derecho como instrumento privilegiado de preservación de las libertades de todo ser humano. Un caso específico que ilustra lo que comentamos es el del llamado "derecho al olvido" en Internet; es decir, el derecho a vigilar y preservar del conocimiento público determinados datos o hechos que afectan a un individuo y éste no desea que sean conocidos. Un buen ejemplo sería el derecho del ciudadano de dirigirse a un motor de búsquedas (Google, Bing…) para solicitarle la eliminación de informaciones desfasadas o no pertinentes por lesivas o dañinas para su persona.

En lo concerniente al "derecho al olvido", no se alude a Internet como medio de comunicación individual de uso restringido (email, chats, foros, Facebook…), donde por definición no se puede ejercer el derecho a la información sobre los contenidos tratados. Por el contrario, el "derecho al olvido" se refiere a Internet como medio de difusión libre de información con acceso público (Web's, blog's, buscadores…), donde sí que se ejerce un derecho a informar prestado por un sujeto con responsabilidad editorial sometido a obligaciones de veracidad. Al respecto, consultar:

Es en este segundo supuesto en el que la sentencia del Tribunal de Justicia de la Unión Europea de 13/5/2014 (asunto C-131/12, Google Spain, S.L., Google Inc. vs. Agencia Española de Protección de Datos) otorgó carta de naturaleza al "derecho al olvido", siendo a partir de entonces cuando la posterior legislación y jurisprudencia está fijando criterios, límites y condiciones para su ejercicio. Como dato cuantitativo que revela el interés ciudadano en esta cuestión, valga como ejemplo el hecho de que, tras la mencionada sentencia, la empresa Google recibió, de mayo a septiembre de 2014, 41.000 solicitudes de retirada de resultados de búsqueda en virtud de las normas europeas de protección de datos.

Sin duda, nuestra sociedad posmoderna y "líquida" al decir del sociólogo Zygmunt Bauman, vive en medio de una paradoja interna: de una banda, el ansia de conexión social constante a través de las redes sociales, lo que conlleva volcar una gran cantidad de datos personales en Internet, muchas veces sin ninguna vigilancia sobre su uso; y, de otra banda, la angustia de que esa pérdida de control sobre los datos, con el paso del tiempo, suponga una grave amenaza para la propia imagen, pudiendo repercutir de forma negativa sobre la valoración social y profesional de la persona individual.

11/09/2017. Las pymes, ante el reto de cumplir con la ley de protección de datos. Las pequeñas firmas llegan a la recta final para la aplicación de la norma con muchos deberes pendientes. FUENTE; abc.es

Las pymes, ante el reto de cumplir con la ley de protección de datos.

Las pequeñas firmas llegan a la recta final para la aplicación de la norma con mucho

Empresas: renovarse o morir

Los datos son el oro de esta nueva era digital. Cuidarlos y darles un buen uso marcará el porvenir y competitividad de las empresas, además de garantizar la seguridad de los ciudadanos. Los ciberataques producidos hace pocos meses por los virus WannaCry y Petya pusieron en alerta a las distintas organizaciones ante posibles robos masivos de datos. Desde entonces no paran de sucederse intentos en todo el mundo –esta semana la empresa de solvencia crediticia de EE.UU. Equifax ha sufrido un ciberataque que ha afectado a 143 millones de sus clientes– y España no ha quedado indemne de sufrir brechas en los sistemas de seguridad, como el ocurrido en la plataforma de comunicación entre los organismos judiciales Lexnet el pasado julio y que supuso que miles de archivos abiertos estuvieran accesibles durante varios minutos.

Sin embargo, no sólo en prevención de seguridad y privacidad actúan las empresas y las administraciones públicas. El nuevo Reglamento General de Protección de Datos (RGPD) impulsado por la UE trae nuevas obligaciones con respecto al reglamento vigente. Aprobado en mayo de 2016, esta nueva ley será aplicable desde el próximo 25 de mayo, por lo que las empresas tienen algo más de ocho meses para ponerse al día en esta materia, donde según el nivel de riesgo de los datos que traten deberán adaptarse a la ley de una manera u otra.

La Agencia Española de Protección de Datos ha creado una herramienta para facilitar a las pymes la adaptación

Según los expertos, el conjunto de las empresas españolas –compuesto en el 99,8% por pymes– todavía tiene tarea por hacer. No cumplir con lo establecido podría acarrear sanciones de 20 millones de euros o, en el caso de las multinacionales, del 4% de la facturación. «El 99% de las pymes tienen menos de 10 trabajadores y es en ese espacio donde se genera un problema gravísimo de papeleos y de temas administrativos. El empresario no suele entender estos temas», explica Antonio Garamendi, presidente de Cepyme, que ve necesario fomentar la formación entre los empresarios.

Con el objetivo de ayudar a las pymes y micropymes a cumplir con la nueva ley, la Agencia Española de Protección de Datos (AEPD) ha presentado esta semana la herramienta «Facilita RGPD». Con ella, las empresas que manejen datos de escaso riesgo –es decir, que no traten datos sensibles, ni esté haciendo perfiles de los clientes ni los use para Big Data– podrán obtener las plantillas que incluyen los requerimientos básicos marcados por el RGPD. Tal y como indica la Agencia, en su registro cuenta con 4,6 millones de ficheros privados inscritos, de los cuales el 75%

de ellos son calificados como de riesgo bajo, cuya responsabilidad en el 90% de los casos recae sobre pymes.

El coordinador de la Unidad de Evaluación y Estudios Tecnológicos de la Agencia,Andrés Calvo, destaca que esta herramienta «aligera trabajo a las empresas» aunque incide en que «el uso de la herramienta no significa el pleno cumplimiento del reglamento». España hasta el momento es el único Estado europeo que ha puesto una herramienta de este tipo y en el próximo plenario del grupo de trabajo de esta materia la ofrecerá al resto.

Los cambios de la ley

Entre las novedades de la nueva ley destaca que los encargados y responsables de los datos deberán llevar un registro de las actividades de tratamiento. Para ello la AEPD recomienda detallar todas las operaciones que se realizan sobre cada conjunto estructurado de datos. Del mismo modo, deberán adaptar las cláusulas informativas –debiendo ser estas mucho más claras– y se elimina el consentimiento tácito.

Pero además de las obligaciones empresariales, los ciudadanos ven reforzados sus derechos. Con la nueva normativa se establece el llamado «derecho al olvido», con el que las personas pueden solicitar a los responsables del tratamiento la supresión de los datos personales cuando haya acabado la finalidad que motivó su recogida. También destaca el derecho a la limitación y de oposición para solicitar al responsable que suspenda el tratamiento de los datos personales.

26/09/2017. Agencia de Protección de Datos avisa a hospitales que deben mejorar la calidad y confidencialidad de datos de pacientes. FUENTE: ecodiario.eleconomista.com (AMPLIAR)

Agencia de Protección de Datos avisa a hospitales que deben mejorar la calidad y confidencialidad de datos de pacientes

La Agencia Española de Protección de Datos (AEPD) ha publicado el 'Plan de Inspección Sectorial de Oficio realizado a Hospitales Públicos' en el que, entre otros aspectos, se avisa de la necesidad de que estos centros sanitarios públicos, gestionados de forma directa o indirecta, mejoren la calidad y confidencialidad de los datos que manejan sobre los pacientes.

Los datos de salud se encuentran incluidos en el Reglamento General de Protección de Datos (RGPD), que será aplicable el 25 de mayo de 2018, entre los catalogados como 'categorías especiales', lo que hace que su tratamiento exija garantías "reforzadas".

Con el diagnóstico de este informe, la AEPD, que ya lo ha presentado a las comunidades autónomas en el marco de la Subcomisión de Sistemas de Información del Sistema Nacional de Salud, ofrece un "punto de referencia" para que el sector sanitario aborde la adaptación de sus sistemas y procedimientos a los nuevos requerimientos que impone el RGPD.

En concreto, el informe está centrado en la auditoría de los aspectos en los que se detectaron carencias en los planes de inspección realizados en 1995 y 2010 y, especialmente, en las medidas de seguridad implementadas.

Para ello, se han auditado hospitales que, partiendo de una situación de historia clínica en papel, la han transferido a formato electrónico; hospitales que conservan todavía la historia clínica en papel y que están inmersos en procesos de automatización, y hospitales que cuentan con historia clínica electrónica desde su creación.

Entre los servicios hospitalarios inspeccionados se encuentran: Admisión, Urgencias, Consultas Externas, Anatomía Patológica, Unidad de Cuidados Intensivos, Laboratorio de Análisis Clínicos, Farmacia Hospitalaria, Departamento de Informática, Atención al Paciente, Servicios Sociales y Biobanco.

De esta forma, y aunque se constata una tendencia "en general favorable" a la progresiva asunción de la normativa y de los principios y cultura de la relevancia que tiene el tratamiento de los datos en el sector sanitario y la debida protección que tienen los mismos.

No obstante, la agencia ha constatado que, respecto a la confidencialidad de los datos, en la mayoría de los centros inspeccionados no se pide al paciente el DNI junto con la tarjeta sanitaria, lo que provoca que se den "casos de suplantación de identidad".

Y es que, aunque la agencia reconoce que hechos así son "muy escasos", pueden suponer un "alto riesgo" para la salud de los enfermos, ya que la información contenida en la historia clínica a la que se accede con la tarjeta sanitaria presentada no corresponde a la patología del paciente.

Asimismo, se ha comprobado que varios de los hospitales analizados no hay carteles informativos en las áreas donde se recaban datos de los pacientes (por ejemplo, en Admisión o Urgencias), no informándose tampoco verbalmente o por escrito sobre los derechos de protección de datos de los pacientes y usuarios del centro.

"Si bien algunos centros hospitalarios sí disponen de carteles informativos sobre los derechos de los pacientes a ser informados, estos no recogen todos los aspectos previstos en el artículo 5 de la Ley Orgánica de Protección de Datos (LOPD), al estar más alineados con la ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, o al tener referencias obsoletas, por ejemplo a la Agencia de Protección de Datos de la Comunidad de Madrid", ha alertado el organismo en el informe.

MEJORAR LA INFORMACIÓN SOBRE LOS ENSAYOS CLÍNICOS

La información sobre los ensayos clínicos también debe de mejorarse o, al menos, así lo considera la AEPD, tras constatar en los contratos con el investigador principal no se especifican aspectos "importantes" como la prohibición de tratar los

datos personales de los sujetos para otrasfinalidades; qué ocurre con los datos al acabar el ensayo; las medidas de seguridad aplicables; así como la obligación de que en las publicaciones de los resultados deba mantenerse la anonimización de los datos.

"Sería recomendable que en el contrato se incluyera la prohibición de tratar los datos personales de los sujetos para otras finalidades distintas a la investigación. Asimismo, sería recomendable especificar qué ocurre con los datos al acabar el ensayo, las medidas de seguridad a aplicar a los datos, y la anonimización de los datos necesaria en las publicaciones de los resultados. El compromiso de confidencialidad debe abarcar sin excepciones toda información que contenga datos personales de los sujetos participantes", ha aconsejado la agencia.

Del mismo modo, se han encontrado consentimientos informados por parte de los pacientes con información "confusa" con respecto a los tratamientos, refiriéndose, por ejemplo, expresamente a datos de salud asociados a datos identificativos, y a que el personal del estudio estará autorizado a revelar esa información a diferentes actores, entre ellos el promotor. Sin embargo, posteriormente, en el cuerpo del documento se indica que los datos comunicados al promotor son "codificados".

También se han encontrado "imprecisiones" como, por ejemplo, que se mantendrá la confidencialidad de los datos "siempre que no sean imprescindibles para el desarrollo del proyecto". Por ello, la agencia ha aconsejado que la información que se facilite a los participantes en un ensayo clínico sea lo "más clara posible y sin ambigüedades".

"Deberá informarse asimismo de las consecuencias especiales de la salida voluntaria del sujeto del ensayo clínico (al revocar su consentimiento) y, en su caso, que los datos recogidos hasta la fecha serán conservados para no desvirtuar la investigación, si bien no se tratarán ni recogerán más datos después de la retirada del consentimiento. Por último, se deberá informar al sujeto sobre la publicación de los resultados de la investigación. En caso de que no sea posible la publicación sin datos identificativos del sujeto, éstos solo podrán ser publicados cuando haya mediado el consentimiento previo y expreso del sujeto", ha detallado.

Para la Agencia Española de Protección de Datos los hospitales públicos también deben reforzar sus medidas de seguridad, potenciando con carácter general los mecanismos de control de acceso. Además, subraya la importancia de preguntar al paciente si desea que su presencia y ubicación en el hospital sea comunicada a las personas o familiares que pregunten por ello y, si éste no se opone, el hospital informe si se encuentra en Urgencias o ingresado y el número de habitación, pero nunca sobre el estado de salud o la atención médica prestada.

Finalmente, el plan va acompañado de un decálogo básico en el que se aconseja tratar los datos de los pacientes como le gustaría que se tratasen los suyos propios; acceder a la historia clínica sólo por requerimiento del trabajo; no dar información a terceros salvo que haya una justificación lícita o el paciente lo haya consentido; cerrar la sesiones de los ordenadores; no enviar información con datos de salud por correo electrónico o por cualquier red pública o inalámbrica y, en el caso de tener

que hacerlo, cifrar los datos; no tirar documentos con datos personales a la papelera; cerrar con llave los armarios que contengan documentación clínica; y no crear por cuenta ajena ficheros con datos personales de pacientes.

02/10/2017. "El objetivo del RGPD es incorporar el cuidado de la información personal al día a día de la filosofía empresarial". FUENTE: tecnología.ederecho.com

"El objetivo del RGPD es incorporar el cuidado de la información personal al día a día de la filosofía empresarial"

- Acaba de incorporarse a Metricson, ¿podría presentarnos brevemente Metricson y cuál es su target de clientes?

Metricson es una firma de servicios jurídicos integrales especializada en negocios tecnológicos y de Internet con sede en Barcelona, Valencia y Madrid. Desde 2009 ayuda a empresas de todo el mundo a desarrollar y proteger su actividad de forma global y con todas las garantías legales.

- Su incorporación va destinada a reforzar el área de IT y Compliance del despacho. Ahondando en ello ¿qué considera que puede aportar su incorporación a la firma?

Mi objetivo principal es situar a Metricson en la punta de lanza de todos los retos tecnológicos y legislativos con los que nos encontramos en la actualidad. La realidad en este sector es tan cambiante y evolutiva que nos obliga a formarnos constantemente y a adaptarnos para poder ofrecer un servicio de calidad a nuestros clientes.

- ¿Por qué el recién publicado Reglamento General de Protección de Datos supone un cambio drástico en el panorama de la privacidad y su protección? En definitiva ¿cuál es su alcance?

El nuevo Reglamento cambia el foco, si la LOPD se centraba en aspectos más formales (ficheros, auditorías bianuales…), el RGPD promueve medidas de evaluación y seguimiento continuas que afectan a todos los trabajadores implicados en el tratamiento de datos. Es decir, se nos va a pedir que acreditemos que nuestra organización mantiene actualizados todos los principios y necesidades que el Reglamento establece, en lugar de la documentación formal debidamente cumplimentada.

Así mismo, se amplía su ámbito geográfico ya que ahora aplica también al tratamiento de datos fuera de la Unión Europea.

Del mismo modo, se refuerza el catálogo de derechos de los usuarios y se amplía el abanico de datos que pasan a ser considerados sensibles, adaptándose así a nuestra realidad actual.

- Se viene constatando desde múltiples instancias y foros la existencia de cierto grado de desconocimiento y pasividad por parte de muchas empresas a la hora de prepararse para la entrada en vigor a pocos meses vista del RGPD. ¿A qué achaca ello?

En mi opinión, esto es debido a que durante mucho tiempo se ha visto la protección de datos como una obligación legal que se debía simplemente acatar para evitar sanciones y no como un elemento más de la cultura y valores de la organización.

El objetivo del RGPD, según el principio de responsabilidad proactiva o accountability por el que se rige, es incorporar el cuidado de la información personal al día a día de la filosofía empresarial, como proceso vivo y en constante evolución.

- ¿Cómo afectará el nuevo Reglamento a las empresas?

Les va a obligar a revisar todos sus procesos, a realizar análisis de riesgos y evaluaciones de impacto para determinar cómo han de adaptarse al nuevo Reglamento y a los nuevos requisitos y figuras que contempla (como por ejemplo, el delegado de protección de datos o DPO). Sin duda se trata de un proceso que debe realizarse de forma progresiva y esmerada, por eso se ha otorgado el plazo de dos años desde la aprobación del texto hasta su obligado cumplimiento.

- Entre sus principales novedades cabe destacar que este Reglamento crea específicamente la figura del Delegado de Protección de Datos (DPO). ¿Considera necesaria una regulación adicional para terminar de perfilar jurídicamente el ámbito competencial, funciones y responsabilidades que ha de asumir esta figura?

Creo que más que perfilar los aspectos que comentas, es necesario definir mejor los requisitos básicos para ser DPO, es decir, determinar cuáles deben ser los conocimientos previos a nivel normativo y del negocio en sí mismo para poder desarrollar satisfactoriamente el trabajo. Desde mi punto de vista, estos requisitos no se han concretado lo suficiente para poder ofrecer garantías tanto a los profesionales como a las organizaciones.

- ¿Considera que el aumento en la cantidad de las sanciones que contempla el Reglamento confiere a este un carácter punitivo y restrictivo?

El incremento intenta ser más un elemento disuasorio que punitivo. El hecho de que afecte a un tanto por ciento del volumen de negocio total anual global del ejercicio financiero anterior, intenta adaptar dicha sanción a la realidad de cada una de las organizaciones y por tanto, que no pueda ser un riesgo fijo cuantificable de base y asumido por la misma.

De esta forma, sobretodo, las grandes corporaciones ven elevado su riesgo proporcionalmente a su tamaño, ajustándose a la realidad de las mismas.

- Acabamos de conocer la multa que la AEPD ha impuesto a Facebook. En este sentido, una vez entre en vigor el RGPD ¿sólo afectará a responsables de actividades de tratamiento de datos personales establecidos en la UE, o también puede alcanzar a los establecidos fuera de la Unión?

Efectivamente, esa es una de las grandes novedades que nos aporta el Reglamento. A partir de ahora los efectos del RGPD no recaerán solo sobre los responsables de fichero y encargados de tratamiento que tengan sede física en la

UE, sino también, y ahí radica la novedad, sobre aquellas organizaciones que aunque no residan en la UE realicen un tratamiento de datos a interesados que sí residan en la UE, siempre y cuando dicho tratamiento esté relacionado con que la oferta del bien o servicio se encuentre en la Unión Europea, o afecte al control de su comportamiento, en la medida que este tenga lugar en la UE.

10/11/2017. El gobierno aprueba el proyecto de la Ley Orgánica de Protección de Datos. FUENTE; Expansion.com

El Gobierno aprueba el proyecto de Ley Orgánica de Protección de Datos

El ministro de Educación, Cultura y Deporte y portavoz del Gobierno, Íñigo Méndez de Vigo, tras la reunión del Consejo de Ministros.

Entre las novedades, se potencia la figura del delegado de protección de datos, persona física o jurídica cuya designación ha de ser comunicada a la autoridad competente, que mantendrá relación con la AEPD.

El Consejo de Ministros ha aprobado el nuevo proyecto de Ley Orgánica de Protección de Datos con el objetivo de aumentar la seguridad jurídica y adaptar la normativa a la evolución tecnológica, además de regular la potestad de los herederos sobre la información de personas fallecidas.

Se trata de una ley que sustituye a la actual y adapta nuestra legislación a las disposiciones del reglamento europeo, introduciendo "novedades y mejoras en la regulación de este derecho fundamental en nuestro país", han asegurado desde el Ministerio de Justicia.

Así, se recogen novedades tanto en el régimen de consentimiento como en los tratamientos y en la introducción de nuevas figuras y procedimientos.

Adelanta a los 13 años la edad -antes 14- de consentimiento para el tratamiento de datos en consonancia con la normativa de otros países.

Además, se toma en cuenta el tratamiento de los datos correspondientes a personas fallecidas en base a la solicitud de sus herederos.

En caso de una inexactitud en los datos personales obtenidos de forma directa, se excluye la imputabilidad del responsable de su tratamiento si éste ha adoptado todas las medidas razonables para su rectificación o supresión.

En las cuestiones relacionadas con el tratamiento de datos, incorpora el principio de transparencia en cuanto al derecho de los afectados a ser informados sobre dicho tratamiento y contempla de forma expresa los derechos de acceso, rectificación, supresión o derecho a la limitación del tratamiento.

Para evitar situaciones discriminatorias, se mantiene la prohibición de almacenar datos de especial protección, como ideología, afiliación sindical, religión, orientación sexual, origen racial o étnico y creencias; en estas categorías, el solo consentimiento del interesado no basta para dar viabilidad al tratamiento.

Igualmente, regula situaciones en las que se aprecia la existencia de interés público, como los relacionados con la videovigilancia o sistemas de exclusión publicitaria.

Entre las novedades, se potencia la figura del delegado de protección de datos, persona física o jurídica cuya designación ha de ser comunicada a la autoridad competente, que mantendrá relación con la AEPD (Agencia Española de Protección de Datos), según explica Efe.

Asimismo, introduce la obligación de bloqueo que garantiza que los datos queden a disposición de un tribunal, el Ministerio Fiscal u otras autoridades competentes (como la AEPD) para la exigencia de posibles responsabilidades derivadas de su tratamiento, evitando que se puedan borrar para encubrir el incumplimiento.

El Reglamento General de Protección de Datos de la UE será de obligado cumplimiento a partir del 25 de mayo de 2018.

07/11/2017. Protección de Datos multa con 300.000 euros a Google por recoger datos personales en Street View. FUENTE: abc.es

Protección de Datos multa con 300.000 euros a Google por recoger datos personales en Street View

La agencia dicta una resolución que pone fin al procedimiento abierto a la empresa de internet en relación a la recogida y tratamiento de datos personales de redes WiFi llevada a cabo por los vehículos empleados en el proyecto hasta 2010

El asunto no es nuevo. Desde 2010 lleva abierto un procedimiento a Google que ahora concluye. La Agencia Española de Protección de Datos (AEPD) ha sancionado con 300.000 euros al gigante de internet al considerar que el gigante de internet «recogió y almacenó datos personales» transmitidos a través de redes WiFi abiertas sin que los afectados tuviesen conocimiento. La información se utilizó para Street View, el servicio que permite explorar en el ordenador lugares de todo el mundo mediante imágenes a pie de calle.

De esta manera, la agencia ha dictado una resolución que pone fin al procedimiento abierto a la empresa Google en relación a la recogida y tratamiento de datos personales de redes WiFi llevada a cabo por los vehículos empleados en el proyecto Street View hasta entonces, dado que la compañía subsanó en su momento el «error». Cabe recordar que la investigación se inició en mayo de 2010. No obstante, la existencia de un procedimiento judicial penal abierto en el Juzgado de Instrucción número 45 de Madrid obligó al regulador español a suspender la tramitación de su procedimiento sancionador en virtud del artículo 7 del Real Decreto 1398/1993, por el que se aprueba el Reglamento del Procedimiento para el Ejercicio de la Potestad Sancionadora. En 2013, sin embargo, la AEPD concluyó la investigación asegurando que el servicio «no vulneraba la normativa española» de protección de datos.

Una vez se tuvo conocimiento de la firmeza del auto por el que se acuerda el sobreseimiento provisional y archivo de las diligencias previas, la agencia ha

reanudado el procedimiento administrativo, resolviéndolo tras el correspondiente plazo de presentación de alegaciones. Según la Ley Orgánica de Protección de Datos (artículo 6.1), el tratamiento de los datos de carácter personal requiere el «consentimiento inequívoco del afectado, salvo determinadas excepciones no aplicables en este caso concreto».

«Hemos colaborado por completo a lo largo de los últimos siete años y, por supuesto, abonaremos la sanción impuesta» (Fuentes de Google)

Fuentes de la compañía norteamericana han explicado a ABC que se trata de un asunto ya solucionado y «no afecta al servicio de Street View actual». «En Google trabajamos concienzudamente para cumplir con las políticas relacionadas con la privacidad. En este caso, y remontándonos al año 2010, ya dijimos públicamente que nos equivocamos e, inmediatamente, informamos del error a la Agencia Española de Protección de Datos y solucionamos el problema que afectaba a nuestros sistemas. Hemos colaborado por completo a lo largo de los últimos siete años y, por supuesto, abonaremos la sanción impuesta», sostienen las mismas fuentes.

En el marco de la investigación realizada, la AEPD ha constatado que Google recogió información de diversa tipología «sin que los afectados tuviesen conocimiento de que dicha recogida» de datos se estaba llevando a cabo y «sin su consentimiento». La compañía recabó, entre otra, información relativa a direcciones de correo electrónico de personas físicas, códigos de usuario y contraseña que permiten el acceso a cuentas de correo electrónico, direcciones IP, direcciones MAC de los routers y de los dispositivos conectados a los mismos o nombres de redes inalámbricas (SSID) configurados con el nombre y apellidos de su responsable. No se ha constatado que Google tratase datos especialmente protegidos a través de estos sistemas, añaden fuentes de la agencia en un comunicado.

En cuanto a que los datos se recogiesen de redes WiFi abiertas, la resolución especifica que «el hecho de que los titulares de redes WiFi no aseguren el cifrado de estas redes, en perjuicio de la seguridad de sus datos, no autoriza en modo alguno la recogida de la información llevada a cabo ni ningún uso posterior de la misma». Recoger y almacenar datos personales sin el consentimiento de sus titulares está considerado infracción graves y castigado con multas de 60.101 a 300.506 euros, mientras que captar datos especialmente protegidos sin autorización o transferir esos mismos datos a EE.UU. sin garantías se considera una infracción muy grave y se multa con entre 300.506 y 601.012 euros.

16/11/2016. Las cofradías tendrán que pedir el consentimiento expreso a los hermanos por sus datos. FUENTE: Sevilla.abc.es (AMPLIAR)

Las cofradías tendrán que pedir el consentimiento expreso a los hermanos por sus datos

El proyecto de Ley, que ya ha sido aprobado en el Consejo de Ministros, contempla al menos tres cambios que afectan en gran medida a las hermandades

La nueva ley de Protección de Datos que entrará en vigor próximamente afectará en gran medida a las hermandades, que tendrán que cambiar su modelo de gestión para evitar incurrir en cuantiosas sanciones en caso de la denuncia de algún hermano. El Consejo de Ministros ha aprobado recientemente el proyecto de ley que, de no sufrir modificaciones, obligará a las corporaciones a que para hacer uso de los datos de los miembros, debe existir el consentimiento expreso de éstos, por escrito. La nueva normativa entró en vigor en 2016 pero el reglamento europeo de protección de datos será plenamente aplicable a partir del 25 de mayo de 2018.

Según ha explicado a ABC de Sevilla el profesor universitario en el CEU Andalucía y experto en Privacidad, Felipe García Pesquera, «hay tres novedades que se aplicarán seguro ya que vienen especificadas por el reglamento europeo».

Menores de edad

Una vez entre en vigor esta nueva ley, los menores de edad con 13 años cumplidos podrán ejercitar el derecho a la protección de datos. Esto supone, por ejemplo, que cualquier niño con esa edad pueda hacerse hermano de una cofradía sin el consentimiento paterno y que, sus padres o tutores, no podrán inscribirlo en ninguna hermandad sin su permiso. García Pesquera señala que esta nueva normativa tiene su raíz en el uso de las redes sociales por parte de los menores y que, según la legislación actual, los menores pueden ejercitar estos derechos con 14 años.

Consentimiento expreso

Quizá sea el principal caballo de batalla en las hermandades en este aspecto en los próximos meses. Hasta ahora, en España se aplicaba el consentimiento tácito a la hora de hacer uso de los datos. Esto, con la nueva ley y el reglamento europeo desaparece. «¿Qué supone esto? Que a partir de ahora, las cofradías tendrán que pedirle a todos sus hermanos que le firmen una autorización para el manejo y cesión de sus datos, como por ejemplo para un censo a un candidato a unas elecciones, al Arzobispado, a la compañía de seguros si son costaleros o, simplemente, para ponerlo en el boletín», afirma el profesor.

Delegado de protección de datos

Otra de las novedades que traerá la nueva ley será la creación de una nueva figura: el delegado de protección de datos, alguien encargado de la privacidad. Será una figura obligatoria en función del volumen de facturación o en el manejo de datos sensibles, como pueden ser los religiosos.

En este sentido, García Pesquera apunta que «no existe todavía ninguna hermandad que esté adaptada a la nueva ley. Sí hay algunas que se adaptaron en su momento a la de 1999, pero esto va a cambiar considerablemente». El próximo mes de enero ofrecerá una charla para los hermanos mayores en el Consejo donde informará de estos asuntos.

«Las hermandades deben trabajar ya en esto porque el próximo 25 de mayo será plenamente aplicable», por lo que el periodo de reparto de papeletas de sitio puede

ser un buen momento para dar a firmar a los hermanos estos consentimientos expresos». indica. No obstante, pese a la importancia del asunto, este profesor aclara que «se trata de un derecho fundamental, personalísimo, sólo esa persona puede ejercitar ese derecho. Es decir, la hermandad sólo se metería en un lío si la denuncia viene de alguien de dentro, no de fuera». García Pesquera concluye afirmando que «lo importante es que empecemos a poner los medios, lo que se conoce como el 'compliance'».

12/12/2017. Aplicaciones infantiles y protección de datos. FUENTE; elperiodico.com

Hay que ajustar aún más los protocolos para proteger a los menores del riesgo de ver vulnerada su intimidad en internet

Uno de cada tres usuarios de internet es un menor, según estimaciones de **Unicef**. De ahí que nunca sean suficientes las medidas para proteger a ese sector de la población de los riesgos de la tecnología digital. Un estudio de unos investigadores de la Universidad de Berkeley advierte, en ese sentido, de la información confidencial, los datos que se facilitan para usar las **aplicaciones infantiles**. Así, destaca que el 8% de ellas obtienen una información exhaustiva de sus usuarios y casi el 50% piden un dato que parece irrelevante, la geolocalización, pero que es un filón en su explotación comercial. Saber en qué barrio vive un niño revela mucho de su entorno familiar. Los menores son, además, un camino ideal para acceder a los padres. Y si los adultos tienen que dar su consentimiento a facilitar datos personales, no suele ocurrir igual con los niños, menos conscientes lógicamente de ello.

El caso de las *apps* infantiles vuelve a poner sobre la mesa la cuestión de la privacidad en internet. Hay que ser conscientes de que representa un bocado muy apetitoso. Bien lo saben las compañías de *data brokers*, que reúnen todo tipo de información sobre los usuarios y hacen negocio con ella con fines publicitarios o incluso políticos. Conviene, por ello, ajustar aún más los **protocolos de protección de datos**, sobre todo con menores de por medio, y reclamar también a la industria que se haga responsable de la situación y revise procedimientos que permiten conseguir datos con tanta facilidad.

BOLETINES AÑO 2017

LA LOPD EN LA EMPRESA

Boletín 01/17

LA LOPD EN EL DÍA A DÍA

¿Cuál es el contenido de una solicitud de derechos ARCO?

Contenido

Cualquier empresa o entidad que trate datos de carácter personal, deberá conceder al interesado un **medio sencillo y gratuito para el ejercicio de los derechos** de acceso, rectificación, cancelación y oposición (ARCO).

El ejercicio de estos derechos será gratuito para el interesado.

El escrito para solicitar un derecho deberá contener lo siguiente:

a) **Nombre y apellidos** del interesado.

b) **Fotocopia del DNI/NIF del interesado,** y en su caso, de la persona que lo representa así como el documento que acredita tal representación.

c) **Petición en que se concreta la solicitud.**

d) **Dirección a efectos de notificaciones**, fecha y firma del solicitante.

e) **Documentos acreditativos** de la petición que formula, en su caso.

No se considerará conforme el envío de **cartas certificadas**, la utilización de servicios de **telecomunicaciones de tarificación adicional**, y cualquier medio que implique un **coste excesivo** para el interesado.

IMPORTANTE

En caso de infracción de la LOPD por una entidad, además de la sanción impuesta por la AEPD, el titular afectado puede exigir también una indemnización

SANCIONES DE LA AEPD

Sanción por control laboral sin comunicación previa a los trabajadores

Antes de realizar cualquier control laboral por el empresario y nunca después, es necesario informar debidamente al trabajador

En el PS/00275/2016 de la AEPD vemos la sanción impuesta a una U.T.E. madrileña a instancias de la UNION GENERAL DE TRABAJADORES **por controlar a sus trabajadores sin informarles previamente.**

En 2015, el sindicato UGT denuncia ante la AEPD a la citada U.T.E. por **proporcionar** a sus trabajadores para el desempeño de su trabajo, **unos dispositivos móviles (PDAs) con línea telefónica y GPS que controla su actividad,** sin haber informado previamente ni a empleados ni tampoco al Comité de empresa.

Este servicio de GPS tiene entre sus fines permitir **el fichaje del personal**, al inicio y al final de la jornada laboral, lo que **indica al empleador la posición exacta del dispositivo, y por tanto del trabajador** a través de las coordenadas (siempre que esté encendido).

En su defensa la UTE declaró que **Sí había entregado tanto a cada trabajador, como al Comité de empresa, documento informativo sobre el tratamiento de dichos datos de geolocalización** de los trabajadores. Sin embargo, **la inspección de la AEPD comprobó** que dicha información al Comité de empresa **se facilitó 2 años después de la recogida de los datos** al comienzo de la actividad que tuvo lugar en el año 2013.

Resultado: multa de 900 € a la U.T.E. MADRID SUR por infracción del art 5 de la LOPD, tipificada como leve en el art 44.2.c) de la misma por no informar en el momento debido.

IMPORTANTE

Los datos de geolocalización se consideran datos de carácter personal, pues permiten fácilmente la identificación del usuario del terminal

LA AEPD ACLARA

Conciliación LOPD y Ley de Transparencia

En el Informe 0178/2014 de la AEPD se plantea la cuestión sobre **cómo interaccionan la LOPD y la Ley de transparencia 19/2013**, y si es posible publicar a través de internet, los datos personales de los beneficiarios con discapacidad de ayudas o subvenciones.

A esta consulta, la AEPD resuelve:

- El objeto de la Ley 19/2013 es **aumentar la transparencia de la actividad pública de la Administración y garantizar el derecho de acceso a la información** sobre su actividad.
- El artículo 5.4 de la Ley 19/2013 señala **que la información que puede ser objeto de transparencia, será publicada en las sedes electrónicas o páginas web** de forma clara, estructurada y entendible.
- Sobre el otorgamiento de subvenciones públicas, es **la propia Ley quien ordena la publicación de cualquier información relativa a actos de gestión administrativa con repercusión económica o presupuestaria (subvenciones, etc.).**
- **Si la información contuviera datos especialmente protegidos** (discapacidad o salud), la publicidad podrá realizarse únicamente:
  - **previa disociación de los datos**
  - **si se cuenta con el consentimiento expreso** y previo del interesado
  - Si la cesión **se encuentra amparada por una norma con rango de Ley**

Fuera de estos tres casos, no sería posible la publicación en internet de datos de beneficiarios de ayudas o subvenciones públicas que tuvieran algún tipo de discapacidad.

IMPORTANTE

Los datos de carácter personal referentes a la salud, solo podrán ser recabados, tratados y cedidos, cuando así lo disponga una Ley o el interesado consienta expresamente

ACTUALIDAD LOPD

La AEPD elabora un decálogo con consejos prácticos de privacidad y seguridad en dispositivos conectados

Fuente: www.agpd.es

La AEPD elabora un decálogo con consejos prácticos de privacidad y seguridad en dispositivos conectados

La Agencia Española de Protección de Datos ha elaborado un listado de claves imprescindibles a tener en cuenta en los dispositivos con conexión a internet.

(Madrid, 15 de diciembre de 2016). Uno de los ejes principales de actuación de la Agencia Española de Protección de Datos (AEPD) es apostar de forma decidida por la prevención para que los ciudadanos sean más conscientes de los derechos que les asisten y cómo ejercerlos. La Agencia ha elaborado un listado de 10 claves imprescindibles en materia de privacidad y seguridad a tener en cuenta en los dispositivos conectados.

1. **Tu cuerpo dice más de lo que crees.** La tecnología 'vestible' (pulseras, relojes, podómetros, etc.) incorpora sensores que registran y pueden transferir información sobre hábitos y costumbres del usuario, tanto al fabricante como a terceros. Si los utilizas para monitorizar tu actividad física, es recomendable comprobar quién está recogiendo los datos que aportas, para qué los va a utilizar y si los va a ceder a otros. Si vas a subir estos datos a una red social intenta dar la menor información personal posible al registrarte y elimina o limita el acceso a tu ubicación siempre que puedas, ya que a partir de este dato se puede inferir mucha más información sobre ti de la que imaginas.

2. **Una ventana indiscreta.** Buena parte de los dispositivos incorporan cámaras que aportan funcionalidades añadidas. Desconéctala o tápala con una cinta adhesiva si no la estás utilizando para evitar que un extraño pueda verte si se hace con el control del dispositivo sin que te des cuenta. Por otro lado, en el caso de un dron, además de la normativa aeronáutica, ten en cuenta que si difundes por internet imágenes en las que se pueda identificar a las personas que aparecen en ellas, necesitarás tener su permiso o consentimiento.

3. **Dispositivos vulnerables.** Bloquea la pantalla de inicio y utiliza un código de desbloqueo lo más largo posible. Además, actualiza el software de tus dispositivos siempre que sea posible para evitar que sean vulnerables ante un posible hackeo y valora instalar algún programa que te proteja ante el software malicioso. Desactiva el bluetooth si no vas a utilizarlo y la conexión automática a wifis abiertas, ya que pueden ser una puerta de entrada para posible ataques.

4. **Protege tus datos ante pérdidas o robos.** Localiza en las opciones de configuración del terminal la forma en la que podrías acceder a distancia a su contenido para eliminarlo y piensa si te interesa utilizar una aplicación para realizar el borrado remoto. Valora si además quieres bloquear algunas aplicaciones que contengan información sensible y, en cualquier caso, realiza copias de seguridad con frecuencia.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_12_15-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Es posible grabar imágenes de alumnos durante el horario de clases?

Debido a la conflictividad alcanzada hoy día en algunos centros docentes, se llega al punto de plantearse por parte de éstos la posibilidad de **instalar videocámaras** no sólo en sus patios, pasillos y zonas de recreo, sino también **dentro de las propias aulas durante el desarrollo de las horas lectivas**.

La cuestión es si conforme a la LOPD, es posible **captar imágenes en un entorno escolar cuando la finalidad es controlar hurtos, acoso escolar o agresiones físicas o verbales a los profesores y compañeros en horario escolar.**

-La instalación de videocámaras en patios, zonas públicas o de acceso a un colegio está permitida y sujeta al ámbito de aplicación de la LOPD y la Instrucción 1/2006, **pues su legitimación se ampara en el art. 2 de la instrucción 1/2006** en relación con el 6.1 de la LOPD y la Ley 23/1992, de 30 de julio, de Seguridad Privada.

-Sin embargo, cuando se plantea si **es posible grabar dentro de las aulas,** la legitimación que existía para el supuesto anterior, no es válida, pues considera la AEPD que su finalidad no es mantener la seguridad del centro sino otra, y por tanto será **necesario el consentimiento de los profesores, alumnos, padres o representantes legales** (si fueran menores de 14 años), **para poder realizar dichas grabaciones**, pues en caso contrario, la grabación sería ilegítima.

IMPORTANTE

Para poder instalar cámaras de vigilancia dentro de las aulas con fines distintos de la seguridad, será imprescindible el consentimiento de los afectados o de sus padres.

LA LOPD EN LA EMPRESA

Boletín 02/17

PRODASUR

LA LOPD EN EL DÍA A DÍA

Relación entre el responsable y el encargado del tratamiento

Uno de los preceptos más importantes de la LOPD es el artículo 12 que regula la figura del **encargado de tratamiento**. Dicho precepto establece que el acceso por un tercero a los datos, cuando sea necesario para prestar un servicio al responsable del tratamiento, **será considerado como un encargo del tratamiento** y no una cesión de datos.

Continúa el artículo estableciendo que **el encargo deberá reflejarse en un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido** y en el que aparezca que dicho encargado sólo tratará los datos conforme a las instrucciones del responsable.

Pero, **¿qué ocurre si el encargado se niega a firmar dicho contrato?**

El RGPD 1720/2007, respecto a esta cuestión, establece que es obligación del responsable **cuando contrate los servicios de un tercero** (asesor fiscal, mantenimiento informático, Hosting, etc.), **comprobar que cumple con toda la normativa de protección de datos personales,** de manera que si esto no es posible, **se recomienda evitar poner los datos personales a disposición de dicho prestador.**

Contenido

IMPORTANTE

En caso de controversia entre las partes, la Agencia Española de Protección de Datos se ceñirá a las pruebas documentales. Cuanto más documentado esté todo, mejor.

SANCIONES DE LA AEPD

Sanción por cesión de datos bancarios y posterior tratamiento sin el consentimiento de su titular

En el PS/00244/2012 vemos la sanción impuesta por la AEPD a un colegio profesional de médicos **por comunicar los datos bancarios de la denunciante a una compañía aseguradora** que gestiona los seguros médicos de los colegiados **y a ésta por tratar dichos datos sin consentimiento.**

Obtener el consentimiento previo es necesario antes de comunicar los datos de una persona a cualquier entidad

Los hechos son los siguientes:

-La denunciante pertenece al Colegio de Médicos de Alicante, responsable del fichero "MÉDICOS" cuyo fin es la gestión administrativa. **Este fichero incluye un número de cuenta bancaria para la domiciliación de la cuota colegial.**

-La entidad aseguradora SEMECO, por su parte, gestiona los seguros médicos del Colegio y **es responsable del fichero ASEGURADOS en el que figura otro número de cuenta bancaria de la denunciante** que fue titular de una póliza de seguro y que anuló devolviendo su recibo.

-Ante tal devolución, SEMECO **volvió a emitir el recibo, pero esta vez a la cuenta bancaria que la denunciante facilitó al COLEGIO** para domiciliar la cuota colegial.

- El COLEGIO DE MEDICOS reconoció comunicar a la aseguradora el número de cuenta y SEMECO que el COLEGIO se la facilitó para emitir el recibo impagado.

RESULTADO: sanción de 6.000 euros al COLEGIO OFICIAL DE MÉDICOS por cesión de datos sin consentimiento (art.11 LOPD) **y de 10.000 € a SEGUROS MEDICOS SEMECO, S.L,** por tratamiento de datos sin consentimiento de los afectados (art. 6.1 LOPD).

IMPORTANTE

El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos

LA AEPD ACLARA

¿Es obligatorio realizar y conservar el informe de auditoría de una empresa?

El RGPD establece en su artículo 96, como medida de seguridad en el tratamiento de datos personales de nivel medio y alto, **la realización de una auditoría que verifique las medidas de seguridad aplicadas** a dichos tratamientos.

El informe 0191/2010 de la AEPD aclara los **plazos de conservación de dichos informes de auditoría.**

De dicho informe jurídico se extrae lo siguiente:

- **A partir de nivel medio,** los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos **cada dos años, a una auditoría** interna o externa.

- Con **carácter extraordinario** deberá realizarse dicha auditoría siempre que se **realicen modificaciones sustanciales** en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. **Esta auditoría inicia el cómputo de dos años** señalado en el párrafo anterior.

- Teniendo en cuenta los plazos de prescripción y de **obligación** de sometimiento a la auditoría, el término durante el cual el **informe debería estar a disposición** de la Agencia Española de Protección de Datos o autoridad autonómica de control competente debería ser el de **dos años**.

- Solo existe la obligación de guardar el **último informe de auditoría**.

IMPORTANTE

No realizar la obligada auditoría en los plazos que marca la Ley es una infracción grave, con sanción de entre 40.001 y 300.000€.

ACTUALIDAD LOPD

La AEPD presenta nuevos materiales para ayudar a las pymes a cumplir con el RGPD

Fuente: www.agpd.es

La AEPD presenta nuevos materiales para ayudar a las pymes a cumplir con el Reglamento europeo de Protección de Datos

La Agencia quiere facilitar que, durante este periodo transitorio, las pymes puedan conocer el impacto que va a tener el Reglamento en la forma en la que tratan datos y las medidas que deben adoptar.

- El Reglamento europeo de Protección de Datos entró en vigor el 25 de mayo de 2016 y será de obligatorio cumplimiento el 25 de mayo de 2018
- Los nuevos materiales incluyen una 'Guía del Reglamento para responsables', 'Directrices para elaborar contratos entre responsables y encargados', y una 'Guía para el cumplimiento del deber de informar', todos ellos incluidos en una nueva sección web específica
- Los recursos han sido elaborados por la Agencia Española, la Autoridad Catalana y la Agencia Vasca de Protección de Datos

Madrid, 26 de enero de 2017. La Agencia Española de Protección de Datos (AEPD) ha publicado hoy nuevos materiales y recursos con los que facilitar a las pequeñas y medianas empresas su adaptación al Reglamento General de Protección de Datos (RGPD), que entró en vigor el 25 de mayo de 2016 y comenzará a aplicarse el 25 de mayo de 2018. Los materiales incluyen una 'Guía del Reglamento para responsables de tratamiento', 'Directrices para elaborar contratos entre responsables y encargados' y una 'Guía para el cumplimiento del deber de informar', todos ellos elaborados junto a la Autoridad Catalana y la Agencia Vasca de Protección de Datos.

La Agencia, en su faceta preventiva, quiere facilitar que, durante este periodo transitorio, las pymes conozcan el impacto que va a tener el Reglamento en la forma en la que tratan datos para que puedan adaptar sus procesos a la nueva normativa, ya que esta supone **un cambio en el modelo de cumplimiento** y exige un compromiso más activo. El objetivo es ofrecer la mayor información posible a las pymes, que suponen el 99% del tejido empresarial español. Los materiales presentados hoy son los siguientes:

Puede ver más información en el siguiente enlace:

https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_01_26_01-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Puede mi vecino colocar una videocámara en la mirilla de su casa para grabar quién transita por el rellano?

En diversas ocasiones se ha planteado la duda de si **es posible que un vecino de una comunidad de propietarios**, por problemas vecinales, o razones de seguridad, **pueda colocar en la mirilla de su puerta, una cámara de videovigilancia que grabe el descansillo** del inmueble y las personas que por él circulan sin su permiso y sin informar al resto de la comunidad.

Según la normativa de protección de datos, **para poder instalar una cámara es necesario**:

-**Respetar el principio de proporcionalidad**

-**Que no se graben espacios públicos**, salvo autorización

-**Informar a los afectados** de que la zona está siendo vigilada y quién es el Responsable ante quien poder ejercer los derechos ARCO

-**Notificar el fichero en la AEPD** salvo que sea emisión en tiempo real.

En la consulta planteada, la captación de imágenes supone un tratamiento de datos sujeto a la LOPD, y como tal, **sólo podrá realizarse con el consentimiento de los interesados o con la autorización de la comunidad de vecinos.**

Si no se cumpliera alguno de estos dos requisitos, la grabación por el vecino sería ilegítima, pudiendo **los afectados solicitar la retirada de la cámara, y en caso de omisión, requerir la tutela de la AEPD**.

IMPORTANTE

Incumplir un requerimiento de la AEPD conlleva la apertura de un procedimiento sancionador penado con sanciones que van desde 40.001 a 300.000 euros

Boletín 03/17

LA LOPD EN LA EMPRESA

LA LOPD EN EL DÍA A DÍA

¿Es Internet una Fuente Accesible al Público según la LOPD?

Contenido

El artículo 3 de la LOPD define las fuentes accesibles al público (FAP) como "**aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación**".

En definitiva, sería toda la información a la que se puede acceder de manera fácil sin tener que pedir permiso a su titular. Además de la definición, este artículo **enumera las fuentes accesibles al público**:

- **El censo promocional**
- **Los repertorios o guías telefónicas**
- **Listas de personas que pertenezcan a grupos profesionales** que sólo contengan el nombre, la profesión, título, actividad, grado académico, dirección profesional e indicación de pertenencia al grupo.
- **Diarios y boletines oficiales**
- **Los medios de comunicación**, como la televisión, la radio, la prensa...

Según la AEPD, cualquier dato personal obtenido a través de un medio diferente, como es **Internet, no será considerado Fuente Accesible al Público,** por lo que para su **tratamiento deberá solicitarse el consentimiento del interesado.**

IMPORTANTE

La AEPD ha determinado en diversos informes y resoluciones sancionadoras que las páginas web no se consideran un medio de comunicación social y por tanto **Internet no es una FAP.**

SANCIONES DE LA AEPD

Sanción por poner cámaras de acceso público

La cuantía de las sanciones podrá graduarse atendiendo, entre otros a la intencionalidad, reincidencia y a los daños y perjuicios causados

En el PS/00048/2010 observamos la sanción impuesta a una conocida cadena de supermercados **por tener colocada una cámara** en la zona de entrada **que capta imágenes de las personas que acceden y las emite en tiempo real, estando disponible su visualización a todo el público.**

En marzo de 2008 entra en la AEPD un escrito de un afectado alegando que el establecimiento **no cumple con la normativa reguladora sobre videograbaciones** y derechos de los ciudadanos.

La cadena de supermercados defiende que las cámaras instaladas tienen como fin controlar los accesos, garantizar la seguridad de clientes y trabajadores de la empresa, así como prevenir hurtos, robos y otros posibles delitos. Además alega que tiene carteles informativos y un contrato de prestación de servicios con la entidad instaladora y de mantenimiento de las videocámaras.

En el Procedimiento de inspección, de las **fotografías aportadas por el denunciante, se observa que la denunciada tiene un monitor a la entrada del establecimiento que reproduce las imágenes captadas, estando disponible su visualización por el público en general** (hecho habitual en muchas entidades). La AEPD determina que **este tratamiento de datos es excesivo y desproporcionado respecto del ámbito y las finalidades que justifican la recogida de dichas imágenes**, y dado que la seguridad se podría haber obtenido por medios menos intrusivos para la intimidad de los afectados, resuelve sancionar al demandado.

RESULTADO: multa de 6.000€por infracción del artículo 4.1 de la LOPD tipificada como grave en el artículo 44.3d) de dicha norma.

IMPORTANTE

Las cámaras podrán colocarse para los fines de control y protección de bienes y personas **siempre que el acceso a las imágenes se limite a usuarios autorizados** y no a todas las personas que accedan al local.

LA AEPD ACLARA

¿Son las ETT y plataformas de búsqueda de empleo Responsables o Encargadas del tratamiento?

El Informe Jurídico 0172/2006 de la AEPD resuelve la consulta sobre **si las empresas de trabajo temporal son consideradas o no encargadas del tratamiento** de datos de las empresas usuarias con las que celebran un **contrato de puesta a disposición de los trabajadores** contratados por aquéllas.

De la consulta se extrae lo siguiente:
-El **trabajador va a quedar sujeto** a la organización y dependencia de la usuaria.
- Las facultades de **dirección y control de la actividad** se ejercen por la empresa usuaria
-Los trabajadores **desempeñan su trabajo en la empresa usuaria**
-**La ETT no va a tener conocimiento de los datos** a los que accede el trabajador, no pudiendo adquirir las obligaciones que impone el art. 12 LOPD
-**La ETT no podrá devolver los datos** al finalizar la relación contractual
-**La ETT no podrá aplicar las medidas de seguridad** correspondientes al tratamiento.

Por tanto, la ETT será una mera intermediaria entre la empresa usuaria y el trabajador, **no teniendo la condición de encargada del tratamiento respecto de los datos de los que sea Responsable la empresa usuaria y a los que accede el propio trabajador**. La comunicación de datos de trabajadores de la ETT a la empresa usuaria **será una cesión de datos** que requiere el consentimiento de sus titulares.

IMPORTANTE

Las ETT o páginas de búsqueda de empleo **deberán recabar el consentimiento de los solicitantes de empleo** titulares de los datos personales para su comunicación a las empresas usuarias finales.

ACTUALIDAD LOPD

La AEPD publica la guía 'Protección de datos y administración de fincas' para facilitar a este sector el cumplimiento de la normativa

Fuente: www.agpd.es

La AEPD publica la guía 'Protección de datos y administración de fincas' para facilitar a este sector el cumplimiento de la normativa

El tratamiento de datos personales en el ámbito de las comunidades de vecinos constituye uno de los motivos de consulta más frecuentes ante la Agencia.

- La información sobre comunidades de propietarios es uno de los temas más consultados en el catálogo de preguntas frecuentes de la página web de la Agencia
- Esta guía forma parte del conjunto de iniciativas adoptadas por la Agencia para facilitar y fomentar el cumplimiento de la normativa de protección de datos
- El documento recoge la aplicación práctica de la normativa de protección de datos vigente, incorporando referencias al Reglamento General de Protección de Datos, que será aplicable a partir del 25 de mayo de 2018

(Madrid, 23 de febrero de 2017). La Agencia Española de Protección de Datos (AEPD) ha publicado la guía 'Protección de datos y administración de fincas', un documento que forma parte del conjunto de iniciativas adoptadas por la Agencia para facilitar y fomentar el cumplimiento de la normativa de protección de datos.

La información referente a comunidades de propietarios es **uno de los temas más consultados** en el catálogo de preguntas frecuentes de la página web de la Agencia. La AEPD considera que publicar una guía orientada a abordar la protección de datos en las comunidades de vecinos a través de los administradores de fincas contribuye tanto a facilitar el trabajo de estos, ofreciéndoles una información ajustada a sus necesidades, como a mejorar el nivel global de protección de los ciudadanos. Según datos del Consejo General de Colegios de Administradores de Fincas, estos gestionan el 80% del parque total de viviendas en España.

'Protección de datos y administración de fincas' aborda en primer lugar **cuestiones generales de la normativa** de protección de datos que se aplican a los administradores de fincas, que actúan por cuenta de las comunidades de propietarios. En este sentido, se incluyen secciones dedicadas a las definiciones de conceptos básicos, a la inscripción de ficheros y el futuro registro de actividades, a la forma de organizar las relaciones entre la comunidad de propietarios y el administrador, y a las principales obligaciones de las partes.

Puede ver más información en el siguiente enlace:
https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_02_23-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Debe un profesional sanitario recabar el consentimiento para tratar los datos de salud de sus pacientes?

Nunca nos cuestionamos si la **recogida de nuestros datos de salud por parte de un centro médico privado, un dentista, una clínica de estética,** etc. requiere de nuestro consentimiento firmado, pues entendemos que con nuestra presencia allí, consentimos dicho tratamiento. Pero, **¿es lícito este tratamiento a efectos de la LOPD**?

La LOPD en su articulado establece como regla general que **los datos referidos a la salud** de las personas **sólo podrán ser recabados, tratados y cedidos,** cuando por razones de interés general **así lo disponga una Ley o el afectado consienta expresamente (mediante una acción que manifieste que realmente está de acuerdo).**

Sin embargo, la propia **LOPD establece como excepción a esta regla general** que podrán tratarse estos datos (sin consentimiento de su titular) cuando sea necesario para la prevención o diagnóstico médicos; para la prestación de asistencia sanitaria o tratamientos médicos; o para la gestión de servicios sanitarios, **siempre que el tratamiento sea realizado por un profesional sanitario.**

No obstante, el GT del artículo 29 señala que esta excepción es válida para prestar al paciente servicios relativos a la salud **a efectos de gestión de servicios de facturación, contabilidad o estadísticas**, **pero no para el tratamiento de los datos de salud** de los pacientes que allí acuden.

Cabe concluir y así lo ratifica la AEPD, **que la regla general para recoger y tratar datos de salud es la que exige el consentimiento libre, inequívoco, informado y expreso de los afectados y así nos lo deberían solicitar todos los centros Responsables del fichero.**

IMPORTANTE

No obstante la regla general del consentimiento, **habrá que respetar lo que indiquen la normativa estatal y autonómica** en lo referente a las historias clínicas.

LA LOPD EN LA EMPRESA

Boletín 04/2017

LA LOPD EN EL DÍA A DÍA

Cómo afecta la LOPD a los datos personales cuando una empresa absorbe a otra

Un hecho que ocurre con frecuencia dentro del ámbito empresarial, es que, ya sea dentro de un grupo de empresas, o bien de forma aislada, **una entidad Responsable de tratamiento se una, compre, absorba o venda su actividad o parte de la misma, a otra empresa.**

Los Responsables se cuestionan que **ocurre en estos casos con los datos de la empresa que cede los datos y que pasan a la nueva**, pues en principio estaríamos ante una cesión de datos personales conforme establece el artículo 11 de la LOPD.

Sin embargo, **el RDLOPD 1720/2007, en su artículo 19** recoge expresamente esta situación, considerándola un "*supuesto especial*", indicando que en los casos en los que se produzca una **modificación del Responsable como consecuencia de una fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad o cualquier operación de transmisión societaria análoga, no se producirá cesión de datos.** Sin embargo, el Responsable de los datos, **deberá informar a los titulares sobre la identidad del nuevo**, dando así cumplimiento al art. 5 LOPD.

Contenido

IMPORTANTE

Los datos de las entidades absorbidas incluidas en los nuevos ficheros, **no implicarán una cesión de datos, sino una simple modificación de la figura del responsable** de la que deberán ser informados los afectados.

SANCIONES DE LA AEPD

Sanción por venta de bases de datos sin cumplir con la Ley

En el PS/00609/2014 de la AEPD podemos ver la sanción impuesta a una entidad **por comercializar bases de datos con direcciones de correo electrónico adquiridas,** a terceras entidades.

De las investigaciones llevadas a cabo por la AEPD deduce:

-Que la **demandada comercializa bases de datos** que dice obtener de fuentes accesibles al público y de páginas Web oficiales de las empresas.

-Que **cada registro contiene**: Identificador, Actividad, Empresa, Dirección, Población, Provincia, CP, Teléfono, Fax, Código CNAE, Descripción CNAE, Código Provincia, Email, Comunidad y también **direcciones de correo electrónico** formadas por nombre y apellidos de los titulares y/o usuarios.

- Que en **las Condiciones Generales del Servicio** de su Aviso Legal **indica que es una empresa dedicada a ofrecer bases de datos de Empresas** para campañas de Marketing.

Dado que **la dirección de correo electrónico es un dato personal sujeto a la LOPD**, cualquier tratamiento del mismo requiere el consentimiento de su titular. Sin embargo, **la demandada no ha podido acreditar el consentimiento previo de los titulares** para **su utilización con fines publicitarios** como consumidores individuales, por lo que la AEPD considera vulnerada la LOPD.

RESULTADO: multa de 50.000€ por infracción del artículo 6.1 de la LOPD tipificada como grave en el artículo 44.3.b) de la misma.

Obtener el consentimiento del interesado es necesario antes de comunicar los datos a una tercera entidad

IMPORTANTE

La dirección de correo electrónico es un dato sujeto a la LOPD en este supuesto **por exceder del ámbito empresarial en el que se enmarcan los ficheros de contactos** de empresa

LA AEPD ACLARA

Comunicación de datos personales de Trabajadores al sindicato solicitante

El Informe 0154/2010 de la AEPD resuelve la consulta sobre **si determinados datos de carácter personal de los trabajadores laborales de un Ayuntamiento pueden ser cedidos a los Delegados Sindicales** de CC.OO de dicho Ayuntamiento conforme a la Ley 15/1999.

-En primer lugar, confirmar que los datos de los trabajadores que se solicitan (nombre y apellidos, fecha de nacimiento, fecha de ingreso, categoría profesional y fecha en que corresponde el primer aumento por antigüedad), **son datos de carácter personal sujetos a la Ley.**

-En segundo lugar, tal y como establece la citada Ley, la comunicación de datos a que se refiere la consulta, **constituye una cesión de datos de carácter personal** que sólo podrá ser realizada con el consentimiento de sus titulares o si una norma con rango de Ley así lo establece.

-La única cesión legal prevista de los datos de los trabajadores sería **la derivada de las funciones atribuidas por el Estatuto de los Trabajadores a los representantes de los trabajadores** (Comité de Empresa, Delegados de Personal o Junta de personal) y solamente en el ámbito de sus competencias, limitándose a los fines de control que a los mismos atribuye el propio Estatuto. El resto de cesiones de datos de los trabajadores, **requerirán consentimiento del interesado.**

Por tanto, sólo será posible la cesión de los datos de los trabajadores solicitados:

- **A los representantes de los trabajadores en el ámbito de sus competencias.**
- **Si se entregan documentos disociados**
- **Si así estuviera recogido en Convenio C.**
- **Con consentimiento de los interesados**

IMPORTANTE

La cesión de datos sin el necesario consentimiento es una de las infracciones más graves en el cumplimiento de la LOPD

ACTUALIDAD LOPD

La AEPD lanza un espacio web para ayudar a los ciudadanos a reclamar sus derechos en materia de telecomunicaciones

Fuente: www.agpd.es

La AEPD lanza un espacio web para ayudar a los ciudadanos a reclamar sus derechos en materia de telecomunicaciones

La Agencia publica esta nueva sección para conmemorar el Día mundial de los derechos de los consumidores que se celebra cada 15 de marzo

- Existen varios organismos competentes en esta materia, por lo que resulta fundamental que el ciudadano sepa ante cuál tiene que presentar su reclamación en función de las circunstancias concretas y cómo debe hacerlo
- Este espacio web forma parte del conjunto de iniciativas adoptadas por la Agencia para fomentar la concienciación de los ciudadanos sobre los derechos que les asisten y cómo ejercerlos
- La sección ha sido elaborada por la AEPD en colaboración con la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital y la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición

(Madrid, 14 de marzo de 2017). Con motivo de la celebración del Día mundial de los derechos de los consumidores el 15 de marzo, la Agencia Española de Protección de Datos (AEPD) ha publicado un espacio web para ayudar a los ciudadanos a reclamar sus derechos en materia de telecomunicaciones.

La creación de esta sección forma parte del conjunto de iniciativas adoptadas por la Agencia para **fomentar la concienciación de los ciudadanos** sobre las garantías y los derechos que les asisten y cómo ejercerlos. Por un lado, una gran parte de las denuncias que recibe la Agencia en asuntos como la inserción indebida en 'ficheros de morosidad' o la contratación irregular tiene relación con el sector de las telecomunicaciones y, por otro, al haber varios organismos públicos con competencias en esta materia, resulta fundamental que el ciudadano conozca ante qué organismo debe presentar su reclamación en función de las causas que la motivan.

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD), la AEPD y los organismos de consumo son las principales entidades públicas con competencias en materia de telecomunicaciones, cada una en sus respectivos ámbitos. Para que el ciudadano pueda obtener una respuesta adecuada a su reclamación es esencial que la plantee ante el organismo adecuado, así como aportar la máxima documentación posible.

La página está dividida en **cuatro espacios**: Qué puedo reclamar y Dónde debo dirigirme; Cómo puedo reclamar; Preguntas frecuentes, donde los ciudadanos encontrarán la respuesta a casos concretos; y Qué documentación tengo que presentar en caso de contratación irregular o fraudulenta, por deudas derivadas de servicios de telecomunicaciones o por inclusión indebida en guías de abonados.

Puede ver más información en el siguiente enlace:
http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_03_14-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Qué es un bitcoin?

Bitcoin es una moneda electrónica o digital que sirve para intercambiar bienes y servicios por internet y que se caracteriza por su eficiencia, seguridad y facilidad de intercambio.

Ventajas que ofrece:

- En Bitcoin **no hay intermediarios** y el dinero pasa directamente de comprador a vendedor o de persona a persona en cualquier momento
- **No es controlado o gestionado por ningún Estado**, banco, institución financiera o empresa. Los usuarios de Bitcoin tienen un completo control sobre su dinero.
- **Es imposible su falsificación** o duplicación.
- Los pagos con Bitcoin son procesados **con tasas bajas o sin tasa alguna**.

Inconvenientes:

- Es un sistema de pago **muy poco conocido**, y por tanto, poco utilizado
- El valor total de bitcoins en circulación y **el número de negocios usando Bitcoin son muy pequeños**
- El desconocimiento conlleva a la **desconfianza por parte de los usuarios**

De cara a la Protección de Datos Personales, es un sistema muy seguro, pues no es necesario revelar la identidad de las partes intervinientes al hacer negocios preservando privacidad de quienes en ellos intervienen.

IMPORTANTE

Para realizar compras con Bitcoins no hay que revelar información comprometida a través de internet, como números de tarjeta de crédito o de cuentas bancarias

LA LOPD EN LA EMPRESA

Boletín 05/17

LA LOPD EN EL DÍA A DÍA

¿Cómo actuar ante un requerimiento de la AEPD?

El RDLOPD establece en su artículo 44.3i) que **no atender a los requerimientos o apercibimientos de la AEPD, o no proporcionar a aquélla los documentos que sean solicitados, se considera una infracción grave.**

Es por ello que en el momento en que tanto el Responsable como la entidad consultora que lo represente, **reciban un comunicado de la AEPD con uno de estos avisos, deberán atenderlo lo antes posible**, respondiendo, rectificando o enviándole la documentación solicitada.

Los requerimientos más habituales son:

-Modificación del contenido de un fichero notificado incorrectamente.

-Justificante de que la consultora que notifica los ficheros está actuando en representación de su cliente.

-Justificante de la subsanación de defectos en las medidas de seguridad denunciados por un afectado.

Modos de atender estos requerimientos:

-Corregir los datos erróneos y notificar de nuevo el fichero.

-Enviar la documentación requerida a la AEPD por correo postal, o a través de cualquier Registro Público

-Enviar la documentación a través de la SEDE ELECTRÓNICA de la AEPD.

Contenido

IMPORTANTE

No atender a los requerimientos de la Agencia Española de Protección de Datos puede conllevar una sanción que oscila entre los 40.001 y los 300.000 euros.

SANCIONES DE LA AEPD

Sanción por vulnerar el deber de secreto y confidencialidad de los datos

En el PS/00599/2016 de la AEPD vemos la sanción impuesta a la entidad NH CENTRAL RESERVATION OFFICE, S.A., **por comunicar datos personales de una empleada al resto de compañeros de trabajo.**

Obtener el consentimiento es necesario antes de realizar una comunicación de datos a un tercero

En enero de 2016, el responsable de RRHH de la entidad NH **envió un correo electrónico a la afectada y por error, en copia, a un grupo numeroso de trabajadores** de la misma en el que se adjuntaba una imagen que contenía el número de la SS, DNI, fecha de nacimiento, número de teléfono móvil personal, tipo de contrato y número de cuenta de cotización a la SS de dicha demandante.

La empleada declara que además, la empresa utiliza el nº de la Seguridad Social como clave de acceso a las nóminas de los trabajadores, por lo que **con los datos que se les ha facilitado, cualquier compañero podía acceder incluso a su número de cuenta corriente.**

Tras realizarse investigaciones por el equipo de la AEPD, se verifica que la entidad **NH no contaba, obviamente, con el consentimiento de la denunciante para la difusión de sus datos** personales produciéndose así una **vulneración del deber de secreto** por parte de la entidad.

RESULTADO: multa de 6.000 € a NH CENTRAL RESERVATION OFFICE, S.A., por una infracción del artículo 10 de la LOPD, tipificada como grave en el artículo 44.3.d) de la misma.

IMPORTANTE

El Responsable y quienes intervengan en cualquier tratamiento de los datos personales de una entidad, están obligados al secreto profesional y al deber de guardarlos

LA AEPD ACLARA

¿Puede la empresa obligar a sus trabajadores a llevar una placa identificativa?

Existen determinadas profesiones de atención al público (camareros, dependientes, comerciales etc.) en las que se requiere la **identificación de sus trabajadores mediante el uso de placas identificativas** en las que figura su nombre, apellidos, DNI, incluso su fotografía, sin el consentimiento del titular.

Algunos trabajadores no obstante, se plantean **si esa práctica puede ser llevada a cabo por las empresas sin vulnerar la LOPD**, pues según esta Ley, los datos de carácter personal sólo podrán ser recogidos y tratados, **cuando sean adecuados, pertinentes y no excesivos** en relación al ámbito y a las finalidades para las que fueron obtenidos.

La AEPD en su Informe 266/2006 responde a esta cuestión **permitiendo este tratamiento** de datos y se basa para ello en otro precepto de la misma Ley que establece que **no será necesario el consentimiento** cuando los datos **se refieran a las partes de un contrato o precontrato de una relación** negocial**, laboral** o administrativa **y sean necesarios para su mantenimiento**.

Por tanto, entiende la AEPD que dado que la finalidad de la identificación es garantizar un trato personalizado con el cliente y cumplir sus funciones laborales, **es posible y adecuado a la Ley 15/1999 llevar dichas tarjetas por los trabajadores** sin pedir consentimiento. No obstante, esto no exime al empleador del deber de informar conforme exige el art.5 Ley.

IMPORTANTE

En la gestión de personal, las organizaciones o empresas deben ser particularmente cautelosas con la recogida de los datos, así como con el deber de informar a sus trabajadores.

ACTUALIDAD LOPD

La AEPD celebrará su 9ª Sesión Anual Abierta el próximo 25 de mayo

Fuente: www.agpd.es

La AEPD celebrará su 9ª Sesión Anual Abierta el próximo 25 de mayo

La Agencia Española de Protección de Datos celebrará, el próximo 25 de mayo, su 9ª Sesión Anual Abierta, que podrá seguirse en directo en streaming a través de la web de la Agencia.

En esta edición se abordarán de manera detallada, entre otros temas, las novedades del Reglamento General de Protección de Datos y, especialmente, su implementación práctica en las organizaciones, así como las actividades realizadas por la Agencia, las novedades legislativas y jurisprudenciales, y los principales retos que afronta este derecho fundamental.

(Consultar el programa completo)

La Sesión está dirigida a representantes de instituciones, empresarios, profesionales de la protección de datos y ciudadanos interesados en la materia. Durante el evento se entregarán los Premios Protección de Datos 2016. Estos galardones, que alcanzan su XX edición, reconocen los trabajos que promueven en mayor medida el conocimiento y la investigación de este derecho fundamental.

El aforo para asistir a la Jornada se encuentra completo. La gestión de las inscripciones ya realizadas puede realizarse a través de la Sede electrónica.

9ª sesión anual

Puede ver más información en el siguiente enlace:
http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_05_05-ides-idphp.php

EL PROFESIONAL RESPONDE

Cumplimiento normativo de una página web

Vivimos en un mundo dominado por las nuevas tecnologías. Las empresas cada vez más **optan por ofrecer sus productos y servicios a través de Internet**, ya sea a través de su web, un blog, o mediante el envío de mailings comerciales.

Sin embargo, poner en marcha un **negocio de venta online,** no sólo consiste en crear la plataforma y exponer los productos, sino que **se deben tener en cuenta también una serie de normas legales** que deben cumplir:

- **Ley Orgánica de Protección de Datos 15/1999**, en cuanto a la obtención y publicación de datos personales que los usuarios proporcionan a través de la web. Es la política de privacidad.
- **Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico** (LSSICE), que establece los trámites necesarios para contratar online. Es el Aviso Legal.
- **Normativa de cookies**, en desarrollo del artículo 22.2 de la LSSICE que establece las obligaciones del prestador del servicio para poder realizar seguimientos de la navegación de los usuarios por la web. Es la política de cookies.
- **Ley General para la Defensa de los Consumidores y Usuarios** aprobado por RD Legislativo 1/2007, establece la información para clientes y usuarios sobre condiciones de contratación a través de la web. Son las Condiciones de Contratación.

IMPORTANTE

Antes de iniciarse el procedimiento de compra on line, deberá ponerse a disposición del usuario una serie de información exigida por la Ley.

LA LOPD EN LA EMPRESA

Boletín 06/17

LA LOPD EN EL DÍA A DÍA

Plazos para atender los derechos ARCO por parte de las empresas Responsables

Establece la LOPD en su articulado que aquellas personas físicas cuyos datos personales estén siendo tratados, **tendrán derecho para ejercitar ante las entidades Responsables del tratamiento los derechos de ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN (ARCO)** sobre dichos datos.

Estos derechos deberán ser **ejercidos bien personalmente por el propio afectado** (debiendo acreditar su identidad), o bien por medio de un **representante legal o voluntario** designado al afecto. Para cumplir con la Ley, las empresas deberán facilitar **medios sencillos y gratuitos**, y deberán atender a los afectados incluso si no disponen de los datos solicitados.

Los plazos para que los Responsables atiendan estos derechos son:

- **ACCESO**: el responsable deberá responder en el plazo máximo de **un mes** desde que recibió la solicitud del interesado.
- **RECTIFICACIÓN y CANCELACIÓN**: **10 días** para rectificar o cancelar los datos incorrectos.
- **OPOSICIÓN**: **10 días** desde la solicitud.

Contenido

IMPORTANTE

Transcurridos los plazos legales sin que el Responsable haya atendido los derechos ARCO, el titular de los datos afectado, podrá solicitar directamente la tutela de la AEPD.

SANCIONES DE LA AEPD

Sanción por incumplimiento de la normativa en materia de protección de Datos

En el PS/00120/2015 de la AEPD, vemos la sanción impuesta a D.A.A.A titular de varios dominios web como consecuencia de la denuncia presentada por una entidad dedicada al desarrollo de páginas web, en la que se declara que el demandado Responsable de fichero, no **cumple con lo dispuesto en la Ley Orgánica 15/1999, y su Reglamento de Desarrollo,** en concreto, que no tiene los ficheros inscritos en la AEPD, que no se recoge consentimiento informado en los formularios ni informa sobre la instalación de cookies de terceros en los equipos de los usuarios.

Obtener el consentimiento es necesario antes de enviar una comunicación comercial vía electrónica

En vista de los hechos denunciados, la Inspección de la AEPD comprueba que:

-**D. A.A.A. es titular** o administrador de varios **sitios web** desde los que recaba datos personales, **no constando fichero alguno inscrito** bajo su titularidad.

-**D. A.A.A. recaba datos** a través de formularios **sin facilitar la información** previa, expresa, precisa e inequívoca que exige el artículo 5.1 de la LOPD.

-**D. A.A.A. utiliza datos personales para enviar comunicaciones comerciales** no solicitadas ni autorizadas previamente.

-**Los sitios web** de D. A.A.A. **instalan cookies sin recabar el consentimiento informado,** ni aparece información alguna relativa al uso y finalidades de las mismas.

RESULTADO: multa de 1.500 € por una infracción del artículo 26.1 de la LOPD, otra de 5.000 € por infracción del artículo 5 de la LOPD, y una tercera de 5.000€ por infracción del artículo 22.2 de la LSSI.

IMPORTANTE

La creación de una página o un dominio web, obliga a su titular a cumplir con la normativa de Protección de Datos (LOPD) y la de Seguridad de la Información (LSSI)

LA AEPD ACLARA

¿Puede considerarse la dirección IP un Dato de Carácter Personal?

El Informe 327/2003 de la AEPD resuelve las cuestiones planteadas sobre si la dirección IP **es un dato de carácter personal y cuál sería el nivel de seguridad aplicable** de conformidad con la Ley Orgánica 15/1999.

1-En primer lugar, la AEPD SI considera las **direcciones IP como datos de carácter personal** sujetas a la LOPD, pues éstas **permiten** a proveedores y administradores de redes, **identificar a los usuarios de Internet** a los que las han asignado sin grandes esfuerzos.

2- Respecto al **nivel de seguridad que corresponde** aplicar a su tratamiento, la AEPD responde que:

-Todos los ficheros con datos personales deben adoptar medidas de seguridad de nivel básico.

-Los ficheros con datos relativos a comisión de infracciones administrativas o penales, los de la Hacienda Pública, servicios financieros, los que se rijan por el artículo 29 de la LOPD, los de la Seguridad Social y los de elaboración de perfiles, deberán reunir, además de las medidas de nivel básico, las medidas de nivel medio.

-Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual o los que contengan datos para fines policiales sin consentimiento del titular, deberán reunir además de las medidas de nivel básico y medio, las de nivel alto.

Por tanto, **al fichero que contenga únicamente direcciones IP, le serán de aplicación medidas de seguridad nivel básico**, pero si se tratan datos de dirección IP asociada a sitios web solicitados para elaborar perfiles de usuario, **evaluando la personalidad del individuo, se deberán adoptar las medidas de nivel medio**.

IMPORTANTE

Los datos personales relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes.

ACTUALIDAD LOPD

La AEPD presenta en su 9ª Sesión Anual Abierta recursos y directrices para facilitar que las pymes cumplan con el Reglamento

Fuente: *www.agpd.es*

La AEPD presenta en su 9ª Sesión Anual Abierta recursos y directrices para facilitar que las pymes cumplan con el Reglamento

La Agencia muestra la versión en pruebas de una herramienta de ayuda para que las empresas que tratan datos personales con un escaso nivel de riesgo puedan estar en disposición de cumplir con las exigencias de la nueva normativa.

- Este recurso práctico, planteado como un cuestionario, se ha ofrecido a asociaciones empresariales y colegios profesionales para que lo evalúen y puedan aportar sus comentarios y sugerencias
- El objetivo de la AEPD es que las pymes obtengan de forma sencilla una lista de medidas que tienen que implantar cuando el Reglamento General de Protección de Datos sea aplicable, el 25 de mayo de 2018
- En paralelo, la Agencia ha publicado hoy la nueva versión de su Guía para el ciudadano, un documento que ya incorpora numerosas referencias al Reglamento, incluyendo las principales novedades respecto al ejercicio de derechos

(Madrid, 25 de mayo de 2017). La Agencia Española de Protección de Datos (AEPD) celebra hoy su 9ª Sesión Anual Abierta, un evento que se ha consolidado como punto de contacto con empresas, organizaciones y profesionales del sector y que también puede seguirse en directo desde la web de la Agencia. Esta 9ª Sesión Anual Abierta se ha centrado en las implicaciones prácticas del Reglamento General de Protección de Datos, cuando falta un año exacto para que la nueva normativa sea de aplicación.

La Agencia ha mostrado hoy durante la Sesión la herramienta de ayuda que está preparando y que está orientada a empresas y profesionales que realicen tratamientos de datos personales de escaso riesgo. Este recurso práctico, planteado como un cuestionario online, se encuentra en fase de pruebas y se ha ofrecido a diversas asociaciones empresariales y colegios profesionales para que lo evalúen y puedan aportar sus comentarios y sugerencias.

El objetivo es que las pymes puedan constatar, en primer lugar, que los tratamientos de datos que llevan a cabo pueden considerarse de bajo o muy bajo riesgo y que, al terminar el cuestionario, obtengan los documentos mínimos indispensables para estar en disposición de demostrar que cumplen con el Reglamento, que será aplicable el 25 de mayo de 2018 (registro de actividades de tratamiento, cláusula informativa y un listado de las medidas de seguridad mínimas, entre otros).

Puede ver más información en el siguiente enlace:
http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_05_25_01-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Qué es el *Compliance*?

Cualquier empresa que hoy día desee conseguir cierto prestigio dentro de un mercado debe **mostrar un alto grado de éxito en el cumplimiento de las normas, tanto de la normativa externa que les viene impuesta, como de las reglas internas de la organización** (políticas internas, compromisos, proveedores, etc.)

La reforma del Código Penal en julio de 2015, introduce una novedad importante, como es, la **responsabilidad penal de las personas jurídicas**, lo que hace necesario que antes de la posible comisión de un delito, la persona jurídica o empresa deba adoptar un modelo de organización y gestión eficaz para prevenir dichos delitos o reducir el riesgo de su comisión**. El conjunto de políticas o medidas que garanticen que una empresa** (incluidos directivos, empleados y agentes relacionados), **cumple con el marco normativo (interno y externo) aplicable, es lo que se conoce como *Compliance*.**

Esta función se puede llevar a cabo por las empresas de dos formas:

- **Establecimiento un modelo de gestión de los riesgos desde dentro de la empresa** con medidas de vigilancia y control para prevenir posibles delitos.
- **De forma descentralizada, contratando los servicios de un profesional especializado** en Compliance.

IMPORTANTE

La introducción de esta medida de control puede aportar un gran valor a la empresa evitando riesgos y contribuyendo a una mejor cultura empresarial.

LA LOPD EN LA EMPRESA

Boletín 07/17

LA LOPD EN EL DÍA A DÍA

Cuándo es lícito el tratamiento de datos personales según el RGPD

Contenido

Las empresas, Administraciones Públicas y cualquier otra entidad a quienes les facilitemos datos de carácter personal, están obligadas a cumplir con unos principios y obligaciones previstos en la Ley Orgánica 15/1999 y su Reglamento de Desarrollo. **A partir del 25 de mayo de 2018, serán de aplicación los principios y obligaciones recogidos por el nuevo Reglamento Europeo de Protección de Datos 2016/679,** el cual establece que **sólo será lícito el tratamiento de datos personales cuando:**

-El interesado haya prestado su **consentimiento previo y explícito**

-El tratamiento sea **necesario para celebrar un contrato** en el que el interesado es parte

-El tratamiento sea necesario **para cumplir con una obligación** impuesta por la Ley a la empresa Responsable

-El tratamiento sea necesario para **proteger intereses vitales** del interesado

-El tratamiento sea necesario para **cumplir una misión (cometido) en interés general o público**

-El tratamiento sea necesario para la **satisfacción de intereses legítimos** perseguidos por el responsable de un tratamiento o por un tercero.

IMPORTANTE

Cada uno de los estados miembros de la UE podrá mantener o introducir disposiciones más específicas para adaptar las normas del nuevo Reglamento a su legislación interna.

SANCIONES DE LA AEPD

Sanción por envío de correos comerciales no solicitados

En el PS/00558/2015 vemos la sanción impuesta por la AEPD a un conocido Centro Comercial **por enviar correos publicitarios a un cliente que no habían sido solicitados**.

El prestador de servicios deberá ofrecer al destinatario la posibilidad de oponerse al envío en cada mensaje remitido

En abril de 2015 tiene entrada en la AEPD escrito del denunciante manifestando que **tras intentar solicitar la baja del servicio en repetidas ocasiones, sigue recibiendo publicidad** y que la **cláusula para darse de baja no funciona.**

Tras solicitar las bajas, el denunciante recibía un correo del Centro Comercial en el que se le indicaba **que no figuraba ningún cliente con su dirección de correo**, solicitándole los datos con los que se registró originariamente en la web.

A la vista de los hechos denunciados, los Servicios de Inspección de la Agencia solicitan información al Centro Comercial y piden al denunciante que reenvíe dos correos electrónicos a éste, para analizar los medios de baja que han sido facilitados.

Al analizarse la cuenta del envío, se comprobó que el denunciante había cambiado el servidor que utilizaba, dando lugar a que el Centro Comercial no pudiera dar de baja **al cliente porque la solicitud contenía un nombre y un sólo apellido, careciendo de datos como la dirección de correo electrónico o dirección postal para ponerse en contacto con él, por lo que no les había sido posible atenderla**. Aun así, la directora de la AEPD acordó iniciar el procedimiento sancionador contra el Centro Comercial.

Resultado: multa de 3.300 € a CARREFOUR por una infracción del artículo 21 de la LSSI, tipificada como leve en el artículo 38.4.d) de la misma.

IMPORTANTE

El tratamiento de datos sin consentimiento, o sin otra habilitación amparada en la Ley, constituye una infracción grave de la LOPD.

LA AEPD ACLARA

Control laboral y derecho a la protección de datos

En el Informe 0464/2013 de la AEPD se plantea si es conforme a la Ley Orgánica 15/1999, la entrega a los trabajadores de una empresa, de un Anexo al contrato de trabajo **informando del deber de secreto y confidencialidad, así como del control del uso de Internet y del correo electrónico** de empresa por parte del empleador

-Respecto al **deber de confidencialidad y secreto,** esta obligación viene establecida en la propia LOPD para todas aquellas personas que intervengan en cualquier fase del tratamiento. Es la empresa Responsable quien está obligada a informar a sus trabajadores sobre este deber. Así pues, **el Anexo al contrato cumple con el deber del responsable de adoptar las medidas necesarias para que el personal con acceso a datos personales conozca su deber de secreto**.

-Junto con el deber de confidencialidad, el Anexo informa también sobre **el control por parte del empleador del uso de Internet y del correo electrónico de empresa por los trabajadores**, facultad prevista en el Estatuto de los Trabajadores frente al derecho a la protección de datos de los trabajadores.

La Sentencia del Tribunal Supremo de 26 de septiembre de 2007, concluye que *"la **utilización de medios que sean propiedad de la empresa** y que ésta facilita al trabajador para cumplir la prestación laboral, **está dentro del ámbito del poder de vigilancia del empresario** debiendo informarse a los trabajadores de que se va realizar dicho control, así como de los medios que van a aplicarse".*

Por tanto, puede hacerlo, pues **mediante la firma del Anexo al contrato de trabajo, la empresa estaría informando al trabajador para que el acceso a los equipos informáticos de los empleados sea lícito por su parte.**

IMPORTANTE

La firma del interesado en un documento es el medio más eficaz con el que el empresario puede probar que informó a sus trabajadores.

ACTUALIDAD LOPD

La AEPD publica una guía práctica para difundir el derecho a la protección de datos entre los ciudadanos

Fuente: www.agpd.es

La AEPD publica una guía práctica para difundir el derecho a la protección de datos entre los ciudadanos

'Protección de Datos: Guía para el Ciudadano' recoge numerosas referencias a los cambios que incorpora el nuevo Reglamento General, que será aplicable el 25 de mayo de 2018, e incluye las principales novedades respecto al ejercicio de derechos.

- Repasa los tradicionales derechos ARCO e incluye otros como el derecho al olvido, el nuevo derecho a la portabilidad, o la forma de solicitar la eliminación de fotos y vídeos en internet y qué hacer en caso de no recibir respuesta
- Contiene ejemplos de los tratamientos de datos que más afectan a los ciudadanos, como ocurre en el caso de las comunidades de vecinos, los llamados ficheros de morosos, la videovigilancia o la publicidad, entre otros

(Madrid, 25 de mayo de 2017). La Agencia Española de Protección de Datos (AEPD) ha presentado 'Protección de Datos: Guía para el Ciudadano' en el marco de la 9ª Sesión Anual de la AEPD, un documento que recoge de forma práctica las claves necesarias para que los ciudadanos conozcan qué derechos les amparan y cómo ejercerlos, y qué obligaciones deben cumplir aquellos que traten sus datos personales. Los datos que maneja la Agencia respecto a las consultas recibidas constatan la importancia que los ciudadanos conceden a la protección de sus datos personales y a su privacidad. Así, en 2016 la AEPD recibió cerca de **237.000 consultas**, casi un 9% más que en 2015. Por su parte, el Barómetro del CIS de febrero de 2017 también destacó esa importancia al señalar que al **76% de los españoles les preocupa la protección de datos personales y el posible uso de su información personal** por terceros.

El Reglamento General de Protección de Datos (RGPD), que comenzará a aplicarse el 25 de mayo de 2018, implica cambios respecto a la normativa actual. Por ello, la Guía para el ciudadano contiene numerosas referencias a la nueva normativa, incluyendo las principales novedades respecto al ejercicio de derechos, detallando qué se puede solicitar en cada uno de los casos.

La Guía repasa los tradicionales derechos de acceso, rectificación, cancelación y oposición (derechos ARCO), la forma de ejercerlos y los plazos legales en los que el ciudadano debe obtenerse una respuesta, incluyendo también aspectos relacionados con **el nuevo derecho a la portabilidad**, en qué consiste y cómo ejercer **el derecho al olvido, o cómo solicitar la eliminación de fotos y vídeos de internet**.

Asimismo, la Guía contiene **ejemplos de los tratamientos de datos que más repercusión pueden tener en los ciudadanos**, como ocurre con los llamados ficheros de morosos, describiendo los requisitos que deben cumplirse para que los datos de una persona puedan ser incluidos en uno de estos ficheros. En este sentido, la inclusión indebida en ficheros de morosidad produce unos efectos especialmente negativos para los afectados, por lo que es imprescindible que las empresas extremen su diligencia antes de comunicar una información inexacta. Por otro lado, el documento recoge otros ámbitos concretos en los que se efectúan tratamientos de datos, como las comunidades de vecinos, la videovigilancia o la publicidad.

Puede ver más información en el siguiente enlace:
http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_05_25_02-ides-idphp.php

EL PROFESIONAL RESPONDE

Riesgos para los datos personales en el uso de Internet

El incremento de servicios de internet, (correo electrónico, buscadores, Redes Sociales, etc.) han logrado grandes avances en los sistemas de información de un tiempo para acá. Sin embargo **esto conlleva posibles peligros a los que se enfrentan sus usuarios**. Para hacer un uso seguro y responsable, los usuarios:

- Deberán **configurar correctamente la privacidad** de su perfil en las redes sociales

- Deberán **proteger su correo electrónico de ataques de ingeniería social** (virus, gusanos y malware en general).

- Deberán **utilizar el campo "Con Copia Oculta"** cuando se envían mensajes de correo a varios destinatarios

- Deberán utilizar **mecanismos que garanticen la confidencialidad** en el intercambio de información

- **Deberán tener precaución con las conversaciones de los chat**, pues los mensajes circulan por equipos de usuarios desconocidos

- **Deberán facilitar a los buscadores sólo los datos necesarios para la prestación de sus servicios** y no más, pues a través de su análisis, pueden realizarse perfiles de hábitos de navegación

- **No deberán publicar información o imágenes de terceros** sin consentimiento

-**No deberán publicar excesiva información personal**, pues podría identificar y localizar al usuario, incluso de forma física.

IMPORTANTE

Internet ofrece grandes ventajas y herramientas que facilitan el trabajo en gran medida, pero también conlleva enormes peligros que podemos y debemos evitar.

LA LOPD EN LA EMPRESA

Boletín 08/17

LA LOPD EN EL DÍA A DÍA

Cuándo es posible tratar datos personales sin consentimiento del titular

El artículo 6 de la LOPD establece uno de los principios básicos en la normativa de protección de datos, estableciendo como regla general que **no será posible el tratamiento de datos personales** (por parte de las empresas) **salvo que se cuente con el consentimiento de su titular o una ley autorice dicho tratamiento.**

No obstante, enumera una serie de **supuestos en los que no será preciso dicho consentimiento**:

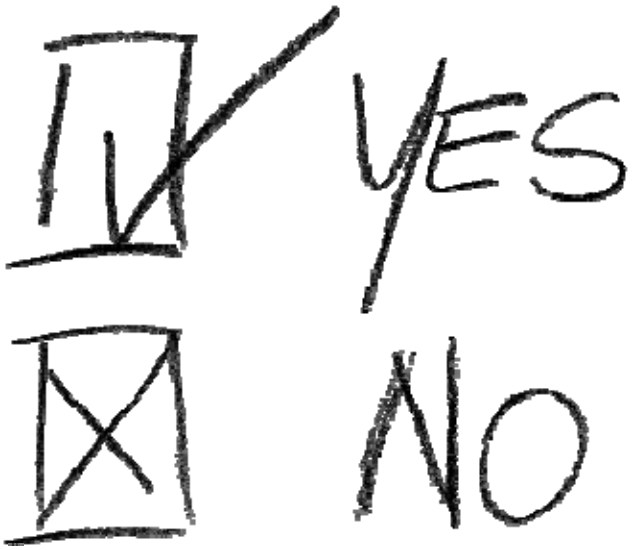
1-Cuando los datos sean recogidos para **ejercer las funciones propias de las Administraciones públicas** (Estado, CCAA, Entidades locales,……).

2- Cuando los datos se refieran a las **partes de un contrato o precontrato de una relación negocial, laboral o administrativa** y sean necesarios para su mantenimiento o cumplimiento.

3-Cuando la finalidad del tratamiento sea **proteger un interés vital del interesado.**

4-Cuando los datos **figuren en fuentes accesibles al público** y su tratamiento sea necesario para satisfacer el interés legítimo del responsable del fichero o de un tercero.

Contenido



IMPORTANTE

A pesar de no ser necesario el consentimiento para tratar los datos en estos supuestos, el Responsable deberá informar en los términos establecidos en el art. 5 de la LOPD

SANCIONES DE LA AEPD

Sanción por incluir datos personales en fichero de morosos

En el PS/00026/2017 de la AEPD vemos la sanción impuesta a **la entidad AIQON por incluir los datos de un interesado en el fichero de morosos Asnef.**

En febrero de 2016, entra en la AEPD escrito de D. A.A.A. denunciando a la entidad de recobro de deuda AIQON por incluir sus datos en ficheros de solvencia patrimonial sin requerirle el pago previo de la deuda.

A la vista de los hechos, la AEPD insta procedimiento de inspección y comprueba:

-Que **existe un fichero de solvencia ASNEF con datos personales de D. A.A.A.** en el que figura como domicilio la C/ALAVA.

-Que la demandada **requirió el pago de la deuda a D.A.A.A con carácter previo** a la inclusión, advirtiendo de su posible inclusión en ficheros de solvencia patrimonial.

-Que existe un **certificado del envío** de la carta remitida a la C/ALAVA en el que se indica que **la carta fue devuelta por motivo de "ausente".**

A efectos de la LOPD y según establece su artículo 4, **es obligación del responsable del fichero que los datos personales que se recojan sean exactos y respondan a la situación actual de los afectados**. Por ello, al conocer que la carta había sido devuelta, AIQON no debió incluir los datos en Asnef sin haberse asegurado su recepción.

RESULTADO: multa de 50.000€ a AIQON por infracción del artículo 4.3 de la LOPD, en relación con el 29.4 de la misma norma y con los artículos 38 y 39 del RLOPD.

Antes de incluir datos personales de clientes en un fichero de morosos, el acreedor deberá informar debidamente al titular de la deuda en los términos que la Ley establece

IMPORTANTE

Constituye una infracción grave tratar datos de carácter personal con conculcación de los principios y garantías del artículo 4 de la LOPD, entre ellos, el de calidad de los datos

LA AEPD ACLARA

¿Puede un empresario instalar un sistema de localización en los dispositivos móviles de sus comerciales?

El Informe Jurídico 0613/2009 de la AEPD versa sobre **si las empresas pueden o no instalar un sistema de geolocalización GPS en los vehículos o en los teléfonos móviles de sus trabajadores** y que son utilizados en su actividad laboral.

Los datos de localización de una persona son Datos de Carácter Personal sujetos a la LOPD, pues identifican a su titular. Pero, **¿hay que pedir el consentimiento a los trabajadores?**

En primer lugar, para poder instalar estos sistemas, **la finalidad deberá ser proporcionada,** no siendo posible si no existe una causa justa. Establece la AEPD que para que sea legítimo el tratamiento de datos de localización de empleados, ha de cumplir unos requisitos:

- Deberá ser una **necesidad de la empresa relacionada con su actividad** (control de transporte de personas o bienes)
- Los datos de localización **han de ceñirse exclusivamente al horario laboral**
- El plazo de conservación de estos datos por el Responsable estará en función de la finalidad de los mismos, y en todo caso, **nunca será superior a los dos meses.** Más allá de ese plazo, el Responsable deberá anonimizarlos.

Si se cumplen estos requisitos, la AEPD considera que **el control laboral del empresario será lícito sin tener que recabar el consentimiento a los trabajadores,** pues se encontraría amparado en el art. 20.3 del ET (debiendo informar debidamente a los mismos).

IMPORTANTE

Además de informar a los interesados, se recomienda informar también a los representantes de los trabajadores sobre los medios de control utilizados por el empresario

ACTUALIDAD LOPD

La AEPD presenta junto a ENAC su Esquema de certificación de Delegados de Protección de Datos

Fuente: www.agpd.es

La AEPD presenta junto a ENAC su Esquema de certificación de Delegados de Protección de Datos

- **La Agencia se convierte en la primera Autoridad europea de Protección de datos que elabora un marco de referencia para esta figura**
- **El objetivo es ofrecer seguridad y fiabilidad tanto a los profesionales de la privacidad como a las empresas y entidades que van a incorporar la figura del DPD a sus organizaciones**
- **Las certificaciones serán otorgadas por entidades acreditadas por ENAC, siguiendo criterios de certificación elaborados por la AEPD en colaboración con los sectores afectados**
- **La elaboración del Esquema ha contado con la participación de un Comité Técnico de Expertos, entre los que se encuentran representantes de sectores y asociaciones profesionales, empresariales, universidades y Administraciones Públicas**

(Madrid, 13 de julio de 2017). La Agencia Española de Protección de Datos (AEPD), en colaboración con la Entidad Nacional de Acreditación (ENAC), ha presentado hoy su Esquema de certificación de Delegados de Protección de Datos. Su elaboración ha contado con la participación de un Comité Técnico de Expertos formado por 23 miembros, entre los que se encuentran representantes de sectores y asociaciones profesionales, empresariales, universidades y Administraciones Públicas. La AEPD se convierte así en **la primera Autoridad europea que realiza un Esquema de certificación de Delegados de Protección de Datos (DPD).**

La AEPD ha optado por promover un sistema de certificación de DPD con el objetivo de **ofrecer seguridad y fiabilidad** tanto a los profesionales de la privacidad como a las empresas y entidades que van a incorporar esta figura a sus organizaciones, ofreciendo un mecanismo que permite certificar que los DPD reúnen la cualificación profesional y los conocimientos requeridos. Las certificaciones serán otorgadas por entidades certificadoras debidamente acreditadas por ENAC, siguiendo criterios de acreditación y certificación elaborados por la AEPD en colaboración con los sectores afectados.

La certificación no es la única vía para ser DPD y en ningún caso será obligatorio utilizar un determinado esquema, si bien la Agencia ha considerado necesario ofrecer un punto de referencia al mercado sobre los contenidos y elementos de un mecanismo de certificación que pueda servir como **garantía para acreditar la cualificación y capacidad profesional** de los candidatos a Delegado de Protección de Datos.

Puede ver más información en el siguiente enlace:
https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_07_13-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Pueden ejercerse los derechos ARCO para dejar de recibir mensajes publicitarios?

El RDLOPD 1720/2007 regula en sus artículos 50 y 51 el ejercicio de los derechos ARCO en relación a los **tratamientos para actividades de publicidad y prospección comercial**. En ellos se establece que:

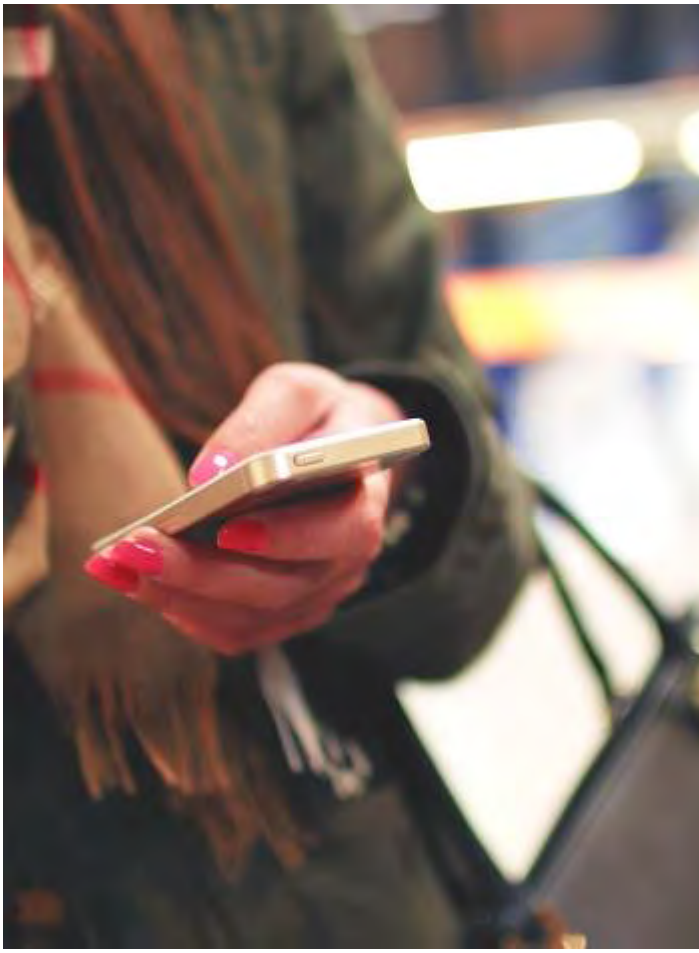
-El Responsable está obligado a **informar** en cada correo **sobre cómo dar cumplimiento** a tales derechos ARCO

-**Si el Responsable encarga a un tercero una campaña publicitaria** y un afectado ejercita los derechos ante el tercero, éste deberá comunicarlo al Responsable para que atienda al afectado en sus derechos.

-**Si los datos personales utilizados para el envío de publicidad se hubieran obtenido de fuentes accesibles al público** en cada comunicación que se dirija al interesado se le informará del origen de los datos, y de la identidad del Responsable.

-Los interesados **tienen derecho en cualquier momento a oponerse al tratamiento** de sus datos con fines comerciales, incluso a pesar de haber sido facilitados por ellos mismos. Este derecho de oposición al tratamiento es **de carácter indefinido**, por lo que **no podrá volverse a enviar comunicaciones comerciales,** salvo que el interesado preste nuevamente su consentimiento.

Por tanto, **el destinatario de los mensajes podrá solicitar en cualquier momento el cese del envío de los mismos. Para ello,** el Responsable deberá facilitarle **un medio sencillo y gratuito,** como puede ser una dirección de correo electrónico o un nº teléfono gratuito.



IMPORTANTE

Podrán enviarse comunicaciones comerciales a personas que figuran en guías públicas, siempre que estos no hubieran ejercido previamente su oposición y se les dé la opción de darse de baja

LA LOPD EN LA EMPRESA

Boletín 09/17

LA LOPD EN EL DÍA A DÍA

Creación y notificación de ficheros públicos

Son ficheros públicos **aquellos cuyos responsables de recoger y tratar datos personales sean las Administraciones Públicas** (Estado, Comunidades Autónomas, Entes Locales y organismos vinculados o dependientes de ellos).

El art. 55 del RDPD dispone al respecto que todo fichero de datos personales deberá ser notificado para su creación, modificación o supresión a la AEPD **por el órgano competente**. Estas notificaciones **deberán realizarse por medio de una Disposición General** (acta o acuerdo de sus miembros de gobierno) **que deberá ser publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente,** y la cual deberá indicar:

a) La finalidad y usos previstos del fichero

b) Las personas o colectivos interesados

c) El procedimiento de recogida de los datos

d) La estructura básica del fichero y la descripción de los tipos de datos a tratar

e) Las cesiones de datos y las posibles transferencias a terceros países

f) Los órganos de las Administraciones que son responsables del fichero.

g) Los servicios o unidades ante los que pueden ejercitarse los derechos ARCO

h) Las medidas de seguridad a aplicar, con indicación del nivel de seguridad exigible.

Contenido

IMPORTANTE

En el plazo de 30 días desde la publicación del acuerdo de creación, Acta o Disposición General, el fichero deberá ser notificado para su registro en la AEPD

SANCIONES DE LA AEPD

Sanción por no atender al requerimiento de la AEPD

El PS/00177/2017 instruido por la AEPD versa sobre la **sanción impuesta a una conocida entidad bancaria por no hacer caso a los requerimientos realizados** para la presentación de cierta documentación.

"Hacer caso omiso a los requerimientos de la AEPD o no proporcionar los documentos solicitados por la misma, son infracciones graves"

-En febrero de 2017 la **Agencia REQUIERE al BANCO BILBAO VIZCAYA ARGENTARIA, S.A. (BBVA) para que aporte unos documentos** sobre una investigación en curso relativa a una denuncia presentada por un cliente del Banco.

-La AEPD comprueba que dicho **requerimiento de información fue fehacientemente notificado** al Banco acreditándose con el acuse de recibo de Correos en el que consta identificada la persona que recogió el requerimiento de información.

-**Transcurrido el plazo** otorgado por la AEPD para contestar al requerimiento **sin que el Banco se hubiera pronunciado**, en abril de 2017 la Directora de la AEPD **acordó iniciar procedimiento sancionador** solicitando nuevamente la información que originó el requerimiento.

- **La Directora de la AEPD decide sancionar al Banco por no contestar al requerimiento inicial** a pesar de que el BBV al fin solicitó posteriormente ampliación de plazo para aportar la documentación requerida.

RESULTADO: multa de 40.001€ al Banco BBVA por no atender los requerimientos de la AEPD según el artículo 45.2de la LOPD.

IMPORTANTE

Ante un requerimiento de la AEPD lo último que debe hacer una entidad es no contestarle. Esta deberá atenderlo en tiempo y forma

LA AEPD ACLARA

Aplicación de la LOPD a una empresa Americana

El Informe Jurídico 0454/2009 de la AEPD resuelve la duda sobre **si es o no de aplicación la vigente LOPD 15/1999 a una empresa con sede en los EEUU** la cual obtiene y trata datos personales (dirección IP, logs, dirección de correo electrónico, cookies..) de usuarios que viven en España y que recaba a través de su página web.

Para fundar la respuesta, la AEPD se remite al artículo 2.1c) de la LOPD que establece que esta Ley será de aplicación a los tratamientos de datos cuando el Responsable del tratamiento **no esté establecido en territorio de la Unión Europea y utilice** en el tratamiento **medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.**

Por tanto, en el caso planteado, sí será de aplicación **la normativa española de protección de datos a la actividad objeto de consulta** pues entiende la AEPD que el responsable del tratamiento (empresa prestadora del servicio con sede en EEUU) **instala cookies y utiliza otras herramientas** como ordenadores, servidores etc.,… **con el fin de recoger y tratar datos personales** que se encuentran en territorio español y no sólo utiliza las redes de comunicaciones como medio de tránsito por los cuales circula la información desde el punto de expedición hasta su destino.

El Grupo de Trabajo del art. 29 considera los ordenadores personales como un medio ubicado en un Estado miembro utilizado para el tratamiento de datos.

IMPORTANTE

Los prestadores de servicios ubicados fuera del EEE que traten datos personales de residentes en España con medios para su tratamiento, deberán nombrar un representante en España.

ACTUALIDAD LOPD

La AEPD convoca los Premios Protección de Datos 2017 de 'Comunicación' y de 'Buenas prácticas educativas para un uso seguro de internet'

Fuente: www.agpd.es

La AEPD convoca los Premios Protección de Datos 2017 de 'Comunicación' y de 'Buenas prácticas educativas para un uso seguro de internet'

Los galardones reconocen aquellos trabajos que suponen una aportación destacada a la difusión de este derecho fundamental.

- La categoría de Comunicación incluye un premio de 3.000 euros y un accésit de 1.500 euros
- Esta edición prioriza los trabajos periodísticos que aborden diferentes aspectos del Reglamento General de Protección de Datos
- El Premio de buenas prácticas educativas se convoca en dos modalidades: una orientada a los centros educativos y otra a personas o entidades que hayan destacado por difundir el uso seguro de internet entre los menores
- El plazo para la presentación de ambas candidaturas finaliza el 31 de octubre de 2017

(Madrid, 1 de agosto de 2017). La Agencia Española de Protección de Datos (AEPD) ha convocado una nueva edición de los Premios Protección de Datos Personales en las categorías de 'Comunicación' y 'Buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet'.

El Premio Protección de Datos Personales de Comunicación 2017, que incluye un premio de 3.000 euros y un accésit de 1.500 euros, tiene por objeto reconocer los **trabajos periodísticos de medios y profesionales de la comunicación** que supongan una aportación destacada a la promoción de este derecho fundamental entre los ciudadanos o que contribuyan a fomentar la concienciación de las entidades que tratan información personal.

Podrán optar a este premio trabajos individuales puntualmente dedicados a la materia objeto de la convocatoria –como un editorial, noticia, reportaje, o programa de radio o televisión– o proyectos periodísticos que definan un compromiso editorial con la promoción de la protección de datos –tales como series de noticias o secciones especializadas–. Los trabajos deben haber sido difundidos entre el **1 de noviembre de 2016 y el 31 de octubre de 2017**.

En esta edición de los Premios de Comunicación se priorizarán los trabajos que aborden **diferentes aspectos del Reglamento General de Protección de Datos**, tanto los relativos a los derechos de los ciudadanos como los que hagan referencia a los cambios en las obligaciones que deben cumplir las entidades que tratan datos personales. Igualmente, se priorizarán los trabajos que hayan contribuido a difundir las **guías, materiales y herramientas realizadas por la AEPD** para concienciar tanto a los ciudadanos como a las entidades sobre la importancia de proteger de forma adecuada la información personal.

Puede ver más información en el siguiente enlace:
http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_08_01-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Qué es el derecho al olvido?

El **derecho al olvido** es el **derecho que tiene el titular de un dato personal a que sea borrada, bloqueada o suprimida toda la información personal que se considere obsoleta por el transcurso del tiempo** y que pueda afectar a alguno de sus derechos fundamentales.

Este derecho en ocasiones choca con la libertad de expresión y de información.

Últimamente se habla mucho de la sentencia del Tribunal de Justicia de la Unión Europea que **obliga a Google a reconocer el Derecho al Olvido** a un ciudadano español al que una noticia del pasado publicada en un medio de comunicación, le estaba dañando su imagen en el presente.

La repercusión internacional ocasionada está generando controversias sobre si este derecho también es aplicado en otros países de la UE, incluso de fuera del EEE.

Para ejercitar el Derecho al Olvido se utilizarán formularios que los propios buscadores han creado para este fin, **debiendo el afectado**:

- Concretar la URL o contenido a eliminar del buscador.
- Identificar al individuo al que se refiere la página web publicada.
- Indicar los motivos por los que se solicita la eliminación de la URL y porqué vulnera su derecho a la protección de datos.

A TENER EN CUENTA

El reconocimiento de este derecho demuestra que la protección de datos también existe en Internet y que las empresas también tienen responsabilidades en este ámbito

LA LOPD EN LA EMPRESA

Boletín 10/17

LA LOPD EN EL DÍA A DÍA

El deber de información y la protección de datos

Es obligación del Responsable del tratamiento informar a los interesados acerca del tratamiento de sus datos.

La vigente LOPD 15/1999 establece que en el momento en que se soliciten los datos del interesado, deberá informarse sobre:

-La existencia del fichero, finalidad y destinatarios.

-El carácter obligatorio o no de la respuesta así como de sus consecuencias.

-La posibilidad de ejercitar los derechos ARCO

-Identidad y dirección del Responsable del tratamiento

El nuevo RGPD 2016/679 exige informar ADEMÁS, de los siguientes aspectos:

-Los datos de contacto del DPD (en su caso)

-La base jurídica o legitimación para el tratamiento

-El plazo o los criterios de conservación de la información

-La existencia de decisiones automatizadas o elaboración de perfiles

-La previsión de transferencias a Terceros Países

-El derecho a presentar una reclamación ante las Autoridades de Control

-Si los datos no se obtienen del propio interesado, el origen de los mismos

-Las categorías de los datos tratados

Contenido

IMPORTANTE

Si los datos se obtuvieron de cesiones legítimas (compras legales), o de fuentes de acceso público (FAP), el Responsable deberá informar a los interesados en el plazo un mes desde que se obtuvieron dichos datos

SANCIONES DE LA AEPD

La AEPD sanciona a Facebook por vulnerar la normativa de protección de datos

En el PS/00082/2017 de la AEPD vemos la sanción impuesta a FACEBOOK **por tratar datos personales incumpliendo varios preceptos establecidos en la LOPD y su Reglamento de Desarrollo.**

En marzo de 2016 la Directora de la AEPD ordena a la Inspección que realice una investigación como consecuencia de una examen de oficio de la citada red social. De dicha investigación se dedujo:

1-**Que FACEBOOK es responsable del tratamiento** de datos de usuarios en la UE
2- Que la LOPD es aplicable al caso, pues FACEBOOK tiene un establecimiento en España: FACEBOOK SPAIN, S.L.
3- Que la red social no cumple con el deber de información facilitada al interesado.
4-Que no se exige al potencial usuario de la red aceptar la política de privacidad en el momento de darse de alta, **careciendo el tratamiento de los datos, de consentimiento**.
5-La herramienta del perfil de usuario de Facebook recoge **datos sensibles (vida sexual, creencias o Salud), sin recabar el consentimiento expreso de su titular**.
6-Tampoco los datos personales de los usuarios son cancelados en su totalidad ni cuando han dejado de ser útiles para el fin para el que fueron recogidos conforme LOPD

RESULTADO: Varias multas a FACEBOOK, entre todas de un millón doscientos mil euros por la infracción de los artículos 6.1, artículo 5, artículo 4, apartados 1 y 2, artículo 7, artículo 4.5, y artículo 16, de la LOPD.

Obtener el consentimiento previo es necesario antes de realizar un tratamiento de datos personales y también antes de enviar comunicaciones comerciales vía electrónica

IMPORTANTE

El órgano sancionador podrá establecer la cuantía de las sanciones según varios criterios: la gravedad, el volumen de tratamientos, la intencionalidad, la reincidencia, etc. beneficios obtenidos

LA AEPD ACLARA

Prevención del Blanqueo de Capitales y LOPD

El informe 0517/2010 de la AEPD resuelve la consulta planteada sobre **cuál es el régimen jurídico aplicable a las cesiones de datos en el seno de los Sistemas Institucionales de Protección SIP (mecanismo de consolidación de Entidades de crédito para su autoprotección), para el cumplimiento de las obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo, en relación a la LOPD.**

De dicho informe jurídico se extrae lo siguiente:

a) El artículo 24 de la Ley 10/2010 traspone al derecho español lo dispuesto en el artículo 28 de la Directiva 2005/60/CE, del Parlamento Europeo y del Consejo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo, cuyo apartado 1 dispone que **las entidades y personas sujetas a lo dispuesto en la presente Directiva, así como sus directivos y empleados, no revelarán al cliente de que se trate ni a terceros que se ha transmitido información** ni que está realizándose o puede realizarse una investigación sobre blanqueo de capitales o financiación del terrorismo.

b) No obstante, la Directiva, dispone que **esta prohibición no impedirá la comunicación entre entidades de los Estados miembros, o de terceros países**, siempre que cumplan las condiciones establecidas en el artículo 11, apartado 1, que pertenezcan al mismo grupo.

En conclusión, **la cesión de datos entre las entidades que conforman un SIP con la finalidad de prevención del blanqueo de capitales y la financiación del terrorismo está amparada por el art. 11.2 a) de la LOPD**, en conexión con el artículo 24.2 a) de la Ley 10/2010 de Prevención de Blanqueo de Capitales.

IMPORTANTE

Los sujetos obligados por esta Ley, aplicarán medidas de seguridad de nivel alto a los tratamientos realizados para cumplir con dichas obligaciones

ACTUALIDAD LOPD

La AEPD presenta Facilita RGPD, una herramienta para ayudar a las empresas a cumplir con la protección de datos

Fuente: www.agpd.es

La AEPD presenta Facilita RGPD, una herramienta para ayudar a las empresas a cumplir con la protección de datos

Con este cuestionario online las empresas y profesionales pueden constatar que los datos que tratan pueden considerarse de bajo riesgo y obtener los documentos mínimos indispensables para facilitar el cumplimiento del RGPD.

- En el acto de presentación la Agencia ha firmado un protocolo de actuación con CEOE y CEPYME para fomentar el conocimiento de la normativa por parte de las empresas
- El Registro de la AEPD cuenta con más de 4,6 millones de ficheros privados inscritos y el 75% de ellos son tratamientos de bajo riesgo cuyos responsables son pymes en más del 90% de los casos
- La AEPD ofrecerá la herramienta al Grupo de Autoridades europeas de Protección de Datos para que puedan utilizarla como base para ofrecer este servicio de ayuda en sus respectivos países

(Madrid, 6 de septiembre de 2017). La Agencia Española de Protección de Datos (AEPD) ha presentado hoy con la colaboración de CEOE y CEPYME Facilita RGPD, una herramienta para **ayudar a las empresas y profesionales que traten datos personales de escaso riesgo a cumplir con el nuevo Reglamento General de Protección de Datos** (RGPD), que será aplicable el 25 de mayo de 2018.

El acto de presentación ha contado con la participación del presidente de CEOE, Juan Rosell; el presidente de CEPYME, Antonio Garamendi, y la directora de la AEPD, Mar España, que han destacado la importancia de ofrecer a las empresas recursos que les permitan adaptarse a la nueva legislación. Asimismo, estas entidades han suscrito un Protocolo General de Actuación para fomentar la difusión del RGPD y de aquellas herramientas, guías y publicaciones realizadas por la Agencia y que puedan ayudar a las empresas en el cumplimiento de sus obligaciones.

Facilita RGPD está planteada como un **cuestionario online con una duración máxima de 20 minutos** con el que las empresas y profesionales pueden, en primer lugar, constatar a través de una serie de preguntas que los datos que tratan pueden considerarse de bajo riesgo y, en segundo lugar, obtener los documentos mínimos indispensables para facilitar el cumplimiento del RGPD al terminar el test.

La información que las empresas aporten –y que la AEPD no conserva ni monitoriza de forma alguna– les permitirá obtener esos documentos casi completados. Esas plantillas incluyen **los requerimientos básicos marcados por el RGPD**, como el registro de actividades de tratamiento, la cláusula informativa, las cláusulas que deberían incluirse si la empresa contrata con un encargado del tratamiento (una gestoría, por ejemplo) y un anexo con las medidas de seguridad mínimas. En la actualidad, el Registro de la AEPD supera los **4,6 millones de ficheros de titularidad privada inscritos** y el 75% de ellos hacen referencia a tratamientos de bajo riesgo (clientes y/o proveedores; nóminas o recursos humanos) cuyos responsables son pymes en más del 90% de los casos.

Puede ver más información en el siguiente enlace:
https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_06-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Tengo que prestar el consentimiento para que mi empresa contrate un seguro o un plan de pensiones?

Existen algunas empresas que contratan **seguros de vida y planes de pensiones en beneficio de sus empleados,** ya sea porque así lo exige su Convenio Colectivo, o como agradecimiento a sus trabajadores por los servicios prestados.

Para poder formalizar estos seguros y/o planes de pensiones, **la empresa debe facilitar a la aseguradora y a los bancos ciertos datos de sus empleados** y en algunos casos, hasta los datos de sus beneficiarios. Pero, **¿puede el empleador contratarlo sin más, o es necesario que cada trabajador preste su consentimiento?**

Siguiendo la regla general establecida en la LOPD, en principio, no podrían comunicarse los datos de los trabajadores y/o sus familiares a la aseguradora y a los bancos sin su consentimiento, pues se estaría vulnerando el artículo 11 de la LOPD. Sin embargo, esta regla general se encuentra exceptuada en una serie de supuestos, uno de los cuales es, **cuando la contratación de este tipo de productos y servicios sea realizada por la empresa en beneficio del trabajador y se base en la existencia de la propia relación laboral.**

En este supuesto concreto, no sería necesario pedir consentimiento a los trabajadores para contratar. No obstante, **es imprescindible que éstos hayan sido informados previamente en los términos establecidos por el artículo 5 de la LOPD** (a quién se ceden los datos y para qué), lo cual puede hacerse bien en el mismo momento de celebración del contrato, o bien mediante una circular informativa posterior.

IMPORTANTE

En la gestión de personal, las empresas deben ser particularmente cautelosas con la recogida de los datos, así como con el deber de informar a sus trabajadores.

LA LOPD EN LA EMPRESA

Boletín 11/17

LA LOPD EN EL DÍA A DÍA

Tratamiento de datos de menores en el nuevo RGPD

Una de las novedades importantes en el nuevo Reglamento Europeo de Protección de Datos es la **obligación de obtener el consentimiento expreso** al recabar datos personales, siendo necesaria una **clara acción o declaración afirmativa, ya sea** mediante el marcado de una casilla en un sitio web, una firma documental, etc.

El artículo 8 del Reglamento establece las **condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información** y dispone que:

1. Será **lícito el tratamiento de datos personales de un niño mayor de 16 años**. Si el niño fuera menor, será necesario el consentimiento del titular de la patria potestad o tutela para tratar sus datos.

2. **Los Estados miembros podrán establecer una edad inferior**, siempre que ésta **no esté por debajo de los 13 años**.

3. El responsable del tratamiento **deberá esforzarse para verificar que el consentimiento fue dado o autorizado** por sus padres o tutores legales.

4. La edad para tratar datos de un menor es independiente de las **normas relativas al Derecho contractual o laboral** de los Estados miembros (como son las normas relativas a la validez o efectos de los contratos en relación con un niño).

Contenido

IMPORTANTE

Hoy día en España, el Real Decreto 1720/2007, mantiene la edad de 14 años para poder tratar datos directamente del menor sin autorización de sus padres o tutores

SANCIONES DE LA AEPD

Sanción por cesión de datos a empresa de publicidad comercial a través de internet

En el PS/00302/2017 de la AEPD, vemos la sanción impuesta a la entidad ENLARED AUTO 10 S.L., dedicada a la venta de automóviles on line por **ceder datos de sus clientes a la entidad LEAD CONVERSION, S.L. (LEAD S.L.) para el envío de correos electrónicos de sus campañas publicitarias sin consentimiento de los titulares**.

Obtener el consentimiento de los titulares es esencial antes ceder datos personales a otra entidad para su propio uso

En octubre de 2016 entra en la Agencia escrito de un afectado que denuncia haber recibido 17 correos electrónicos con información comercial sobre productos y servicios de telefonía, seguros de salud, viajes y alojamientos, muebles remitidos desde una cuenta perteneciente a la entidad LEAD S.L. que no han sido solicitados o autorizados previamente por él.

La AEPD inicia la investigación **requiriendo a LEAD S.A. que le informe sobre el origen de la dirección de correo del denunciante y el consentimiento para el envío** de comunicaciones comerciales.

LEAD aporta copia del contrato con ENLA REDAUTO 10, S.L. en el que se establece la prestación de servicios de intermediación comercial autorizándole **a LEAD S.L. para que designe los destinatarios finales de todas sus campañas.**

El denunciado, responsable del tratamiento de los datos del denunciante **ha realizado una comunicación de datos de direcciones de correos electrónicos a LEAD, S.L. para su propio uso y beneficio sin poder acreditar el consentimiento** de los interesados.

RESULTADO: multa de 3.000 € a ENLARED AUTO 10, S.L., por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.b) de la LOPD de conformidad con lo establecido en el artículo 45 apartados 2 y 5 de la citada LOPD.

IMPORTANTE

Es obligación del responsable del tratamiento poder demostrar que recabó el consentimiento de los interesados antes de comunicar los datos a un tercero

LA AEPD ACLARA

Ley de Transparencia y Protección de Datos

El Informe Jurídico 0178/2014 de la AEPD plantea varias cuestiones relativas a **cómo afecta la Ley 15/1999 a la aplicación de la Ley 19/2013, de transparencia,** acceso a la información pública y buen gobierno.

La Ley 19/2013 **regula el derecho de acceso a la información pública por parte de todos los ciudadanos,** la cual será publicada en las correspondientes sedes electrónicas o páginas web de las distintas Administraciones Públicas.

En dicha información se **encontrarán publicados datos de carácter personal de los obligados y otras personas físicas.**

¿Cómo afecta esto a la protección de Datos?

-Los datos de personas que se hagan públicos, **estarán sometidos a la LOPD.**

-Su publicación o cesión en la web **está legitimada en el art. 11.2 a) de la LOPD**, pues la publicación de información está prevista en la Ley de Transparencia 19/2013, que no sólo la autoriza, sino que establece los criterios que regirán dicha publicidad.

-Si esa información **contiene datos de salud (de beneficiarios de subvenciones,** por ejemplo), **deberá procederse a su disociación**, a menos que se cuente con el consentimiento previo.

-Podrá ejercitarse el derecho de acceso a los datos, pero teniendo en cuenta otras leyes referidas al derecho de información.

-La normativa de protección de datos será de aplicación al tratamiento posterior de los datos obtenidos a través de dicho derecho de acceso

IMPORTANTE

Los datos de carácter personal objeto del tratamiento, podrán ser tratados sin el consentimiento de su titular cuando la cesión esté autorizada o prevista en una ley.

ACTUALIDAD LOPD

La AEPD sanciona a Google por tratar sin consentimiento datos personales recogidos a través de redes WiFi con los coches de su servicio Street View

Fuente: www.agpd.es

La AEPD sanciona a Google por tratar sin consentimiento datos personales recogidos a través de redes WiFi con los coches de su servicio Street View

La Agencia constata que Google almacenó datos personales transmitidos a través de redes WiFi abiertas sin que los afectados tuviesen conocimiento de dicha recogida.

- La Agencia ha constatado que Google captó y almacenó sin consentimiento datos personales de los ciudadanos procedentes de redes inalámbricas a través de los vehículos empleados en su proyecto Street View
- El procedimiento declara la existencia de una infracción grave de la Ley de Protección de Datos e impone a Google una sanción de 300.000 euros
- La AEPD se vio obligada a dejar en suspensión la tramitación de este procedimiento administrativo en 2010 tras la presentación de una denuncia por la vía judicial penal, resolviéndolo una vez adoptada la resolución judicial

(Madrid, 7 de noviembre de 2017). La Agencia Española de Protección de Datos (AEPD) ha dictado una resolución que pone fin al procedimiento abierto a la empresa Google en relación a la recogida y tratamiento de datos personales de redes WiFi llevada a cabo por los vehículos empleados en el proyecto Street View. En el marco de la investigación realizada, la AEPD ha constatado que Google recogió y almacenó datos personales transmitidos a través de redes WiFi abiertas sin que los afectados tuviesen conocimiento de dicha recogida y sin obtener el consentimiento de los mismos. En consecuencia, la Agencia **declara la existencia de una infracción grave** e impone a Google una sanción de 300.000 euros.

La AEPD inició de oficio la investigación de estos hechos en mayo de 2010. No obstante, la existencia de un procedimiento judicial penal abierto en el Juzgado de Instrucción Nº 45 de Madrid obligó a la AEPD a suspender la tramitación de su procedimiento sancionador en virtud del artículo 7 del Real Decreto 1398/1993, por el que se aprueba el Reglamento del Procedimiento para el Ejercicio de la Potestad Sancionadora. Una vez se tuvo conocimiento de la firmeza del auto por el que se acuerda el sobreseimiento provisional y archivo de las diligencias previas, la Agencia Española de Protección de Datos ha reanudado el procedimiento administrativo, resolviéndolo tras el correspondiente plazo de presentación de alegaciones.

La Ley Orgánica de Protección de Datos establece en su artículo 6.1 que el tratamiento de los datos de carácter personal **requiere el consentimiento inequívoco del afectado**, salvo determinadas excepciones no aplicables en este caso concreto. En el marco de la investigación realizada, la Agencia Española de Protección de Datos ha constatado que **Google recogió información de diversa tipología** sin que los afectados tuviesen conocimiento de que dicha recogida de datos se estaba llevando a cabo y sin su consentimiento. La compañía recabó, entre otra, información relativa a direcciones de correo electrónico de personas físicas, códigos de usuario y contraseña que permiten el acceso a cuentas de correo electrónico, direcciones IP, direcciones MAC de los routers y de los dispositivos conectados a los mismos o nombres de redes inalámbricas (SSID) configurados con el nombre y apellidos de su responsable. No se ha constatado que Google tratase datos especialmente protegidos a través de estos sistemas.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_11_07-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Qué es una Evaluación de Riesgos?

Como consecuencia del desarrollo de la tecnología, **los datos de carácter personal adquieren cada día un mayor valor económico para las empresas,** siendo necesaria la **adopción de nuevas medidas que contribuyan a su protección** y por tanto, al respeto de los derechos de las personas.

Para ello son útiles algunas herramientas nacidas a raíz de la nueva legislación europea sobre Protección de Datos como las **"Evaluaciones de Impacto en la Privacidad" (EIPD).**

Una EIPD consiste en:

1- La **realización de un análisis de los riesgos** que un determinado sistema de información, un producto o servicio que va a salir al mercado, puede suponer para el derecho fundamental a la protección de datos

2- **Tras ese análisis, se ha de llevar a cabo una gestión eficaz** de los riesgos que se hubieran identificado

3- Una vez identificados**, se deberán adoptar las medidas necesarias para eliminarlos o mitigarlos**

Una EIPD se requerirá en caso de que las empresas lleven a cabo tratamientos de:

- **Elaboración de perfiles** y análisis automatizado de aspectos personales de individuos
- **Categorías especiales de datos** personales a gran escala
- **Observación sistemática de zonas de acceso público** a gran escala

IMPORTANTE

El informe final de la EIPD debe ser remitido a la alta dirección de la empresa para que tome las decisiones necesarias sobre las medidas sugeridas por el equipo

LA LOPD EN LA EMPRESA

Boletín 12/17

LA LOPD EN EL DÍA A DÍA

Cuándo es necesario nombrar un DPO en la empresa

Una de las novedades importantes que introduce el nuevo RGPD (UE) 2016/679, de 27 de abril de 2106, cuya entrada en vigor está prevista para el 25 de mayo de 2018, es la designación o contratación de una **figura encargada de informar y asesorar a los Responsables y encargados del tratamiento acerca de las obligaciones para cumplir con dicho Reglamento**. Es la figura del DPO o Delegado de Protección de Datos

La cuestión que genera gran inquietud es si **todas las entidades necesitan nombrar a esta figura o sólo alguna en particular**.
El art. 37.1 del RGPD establece de forma expresa que el responsable y el encargado del tratamiento designarán un DPD siempre que:

a) **el tratamiento de datos sea realizado por una autoridad u organismo público**, excepto los tribunales cuando actúen en ejercicio de su función judicial

b) las actividades del responsable o del encargado consistan en **tratamientos de datos que requieran una observación habitual y sistemática de interesados a gran escala** (videovigilancia a gran escala)

c) las actividades del responsable o del encargado consistan en el **tratamiento a gran escala de categorías especiales de datos personales e infracciones penales**

Contenido

IMPORTANTE

El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

SANCIONES DE LA AEPD

Sanción por recoger datos de menores sin consentimiento

En el **PS/00339/2011** de la AEPD vemos la sanción que sufre una entidad por **recoger datos de menores de edad sin obtener el consentimiento paterno previo.**

Las entidades responsables deberán establecer procedimientos para recoger datos personales y ejercer los derechos ARCO.

Con fecha 1 de febrero de 2011 se recibe en el registro de la Agencia Española de Protección de Datos escrito de reclamación de D. A.A.A., en el que pone de manifiesto que durante el mes de diciembre de 2010 y comienzos de enero de 2011, **el canal infantil de televisión TDT BOING** promocionaba la **asistencia a la Cabalgata de Reyes** en una carroza patrocinada por la cadena. **Para participar** en el concurso, **se debía cumplimentar un formulario disponible en la web www.boing.es**, el cual recogía datos personales de menores puesto que en las bases de la promoción figuraba que iba dirigido a niños entre 7 y 12 años. No obstante**, no se solicitaba el consentimiento del tutor legal ni se facilitaba claramente la finalidad de la recogida ni la información necesaria para ejercitar los derechos ARCO.**

En la inspección de la AEPD se comprueba que **aunque el sitio web www.boing.es es un portal dirigido a un público juvenil cuya información facilitada en la recogida de datos se realiza cumpliendo la LOPD**, sin embargo, **en la recogida de datos para participar**, en fechas del 15 de diciembre hasta el 26 de diciembre de 2010, en la promoción de la Cabalgata de Reyes en Madrid para menores entre 7 y 12 años, era necesario **rellenar un formulario con datos personales, no existiendo ninguna opción para solicitar la autorización** del padre/madre/tutor, **ni constaba la información establecida por la LOPD**.

Resultado: Sanción de 20.000 € por una infracción del artículo 6.1 de la LOPD

IMPORTANTE

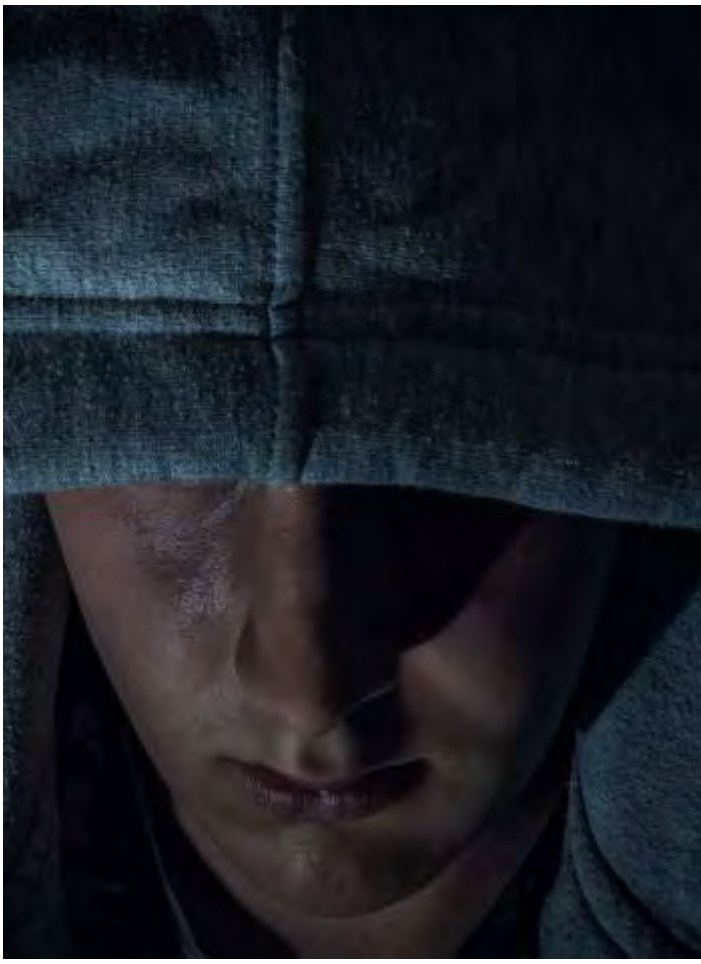
Se ha de ser especialmente cauto a la hora de recoger y tratar datos personales y especialmente de menores de 14 años

LA AEPD ACLARA

Puede una empresa solicitar a un demandante de empleo certificado de antecedentes penales?

El Informe Jurídico 0401/2015 de la AEPD resuelve sobre **si puede una empresa solicitar el certificado de antecedentes penales o el certificado negativo del Registro Central de delincuentes sexuales** a aquellas personas que pretenden acceder a puestos de trabajo en ella, de conformidad con la LOPD.

Para aclarar esta cuestión es necesario valorar la actividad de la empresa y cada puesto de trabajo concreto. Existen dos posibilidades:



-Si se pretende acceder y ejercitar **profesiones, oficios o actividades que impliquen contacto habitual con menores**, el requerimiento de los datos en cuestión, **estaría legitimado por ley**, pues la LO1/1996, de Protección Jurídica del Menor, modificada en 2015, establece como requisito para acceder y ejercitar dichas profesiones, no **haber sido condenado por sentencia firme por algún delito contra la libertad e indemnidad sexual** y por tanto, quien pretenda el acceso a tales profesiones deberá acreditar esta circunstancia aportando una certificación negativa del Registro Central de delincuentes sexuales.

-Ahora bien, **en el caso de que no sea necesario el contacto habitual con menores para el desempeño de la actividad** o puesto solicitado, no resultará posible exigir dicho certificado, pues el tratamiento de estos datos no tiene habilitación legal, pudiendo ser tratados estos datos solamente por la Administración Pública.

IMPORTANTE

Los datos personales relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas

ACTUALIDAD LOPD

El Esquema Nacional de Seguridad recoge las medidas que debe aplicar el sector público para cumplir con los requisitos del RGPD en este ámbito

Fuente: www.agpd.es

El Esquema Nacional de Seguridad recoge las medidas que debe aplicar el sector público para cumplir con los requisitos del RGPD en este ámbito

El CCN-CERT y la AEPD establecen un mecanismo de colaboración para ofrecer a las Administraciones Públicas una referencia de cumplimiento normativo en materia de protección de datos y seguridad.

- La herramienta PILAR para Administraciones Públicas incluye desde hoy un módulo para facilitar el cumplimiento
- El Reglamento General de Protección de Datos (RGPD), que establece nuevos requisitos, será aplicable el 25 de mayo de 2018

(Madrid, 12 de diciembre de 2017). El CCN-CERT y la Agencia Española de Protección de Datos (AEPD) han establecido un mecanismo de colaboración con el objetivo de ofrecer a las Administraciones Públicas una referencia de cumplimiento normativo en materia de protección de datos y seguridad ante la próxima entrada en vigor del Reglamento General de Protección de Datos (RGPD) el 25 de mayo de 2018.

El Esquema Nacional de Seguridad y el RGPD establecen la obligación de que las Administraciones Públicas realicen análisis de riesgos para determinar el posible impacto de los tratamientos de datos sobre los derechos y libertades de las personas y las medidas de seguridad aplicables.

En este sentido, la AEPD ha publicado un documento en el que pone de manifiesto que esas medidas de seguridad –en el caso de las AAPP– estarán marcadas por los criterios establecidos en el Esquema Nacional de Seguridad. El Proyecto de Ley Orgánica de Protección de Datos, actualmente en fase de tramitación, lo recoge de la misma forma en su disposición adicional primera.

Fruto de la colaboración, el CCN-CERT y la AEPD han trabajado de forma conjunta para ofrecer una herramienta a las Administraciones Públicas que les permita evaluar de manera sistemática y objetiva los posibles riesgos en materia de protección de datos y de seguridad de la información. Así, la herramienta PILAR incluye desde hoy un módulo de cumplimiento que permite a las AAPP verificar los requisitos establecidos en el RGPD, facilitando la gestión normativa tanto del Reglamento como del Esquema Nacional de Seguridad.

La obligatoriedad de contar con un registro de actividades de tratamiento, designar un Delegado de Protección de Datos o notificar las quiebras de seguridad en caso de producirse son algunos de los aspectos recogidos en este nuevo módulo.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_12_12-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Pueden incluirme en un grupo de WhatsApp sin mi permiso?

La creación de un grupo de **WhatsApp por una entidad pública o privada, tiene relación directa con la protección de datos personales**, pues en el momento en el que alguien te agrega a dicho grupo, tanto tu número de teléfono, como tu foto de perfil, serán accesibles por el resto de personas que lo forman, algunas de las cuales, quizás ni siquiera conoces.

A efectos de la LOPD **esto es considerado una cesión de tus datos personales**, para lo que legalmente **es preciso el permiso o consentimiento del titular de los datos**.

La Agencia Española de Protección de Datos (AEPD) acaba de dictar una resolución en la que analiza esta situación y concluye con la **existencia de varias infracciones**:

- **Tratamiento de datos de carácter personal sin recabar consentimiento de** los afectados
- **Revelación de datos personales** infringiendo el deber de secreto al que está obligado el responsable
- **Tratamiento de datos para fines diferentes** para los que los mismos fueron recabados
- **Cesión de datos sin contar con el consentimiento del interesado**

Por ello, **antes de crear un grupo de WhatsApp**, salvo que tenga fines personales o domésticos, **deberá ser aceptado por todos sus componentes**.

IMPORTANTE

La creación de un grupo de WhatsApp tiene también un marco legal que respetar, al menos en materia de protección de datos personales

.PROTECCION DE DATOS Personales

Servicio de consultoría, para el cumplimiento de la Ley Orgánica de Protección de Datos de caracter personal 15/1999 orientado a la empresa, para que con un mínimo esfuerzo cumplamos con las obligaciones derivadas de la actual Ley Orgánica de Protección de Datos y normativa de desarrollo vigente.

Nuestro Servicio cubre todas las necesidades de su empresa:

- **Estudio Previo**.
- **Inscripción ficheros** en la Agencia Española de Protección de Datos.
- **Documento de Seguridad** personalizado.
- **Legitimación documentos: Contratos empresa-asesor**, captura de datos, cartas confidencialidad...
- **Formación presencial y/o a distancia** al personal.
- **Revisiones anuales** para la actualización de los protocolos y controles periódicos.
- **Auditoría bienal obligatoria**.
- Adecuación a la **LSSICE** (Ley 34/2002).
- **Servicio de Atención Telefónica**, asesoramiento legal y soporte jurídico permanente.

  Emisión **certificación** de adecuación LOPD.

NO DEJE PASAR ESTA NUEVA OPORTUNIDAD

Llamenos al

902 15 22 25

PRODASUR

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