



2^a
sesión
anual
abierta
de la AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



CONSULTAS DE LOS ASISTENTES

JESÚS RUBÍ NAVARRETE
Adjunto al Director de la AEPD

¿Quién autoriza la publicación de una esquila de un difunto y, por tanto, los datos contenidos en ella?

- La LOPD no se aplica a los datos de personas fallecidas
- La publicación de datos en la esquila del difunto cuando la realizan personas físicas puede considerarse como un tratamiento de la información realizado en el marco de la vida privada o familiar de los particulares, al que tampoco se aplica la LOPD.

¿Qué criterio tiene la AEPD sobre la consideración como dato de carácter personal de los teléfonos móviles o las direcciones IP después de la SAN de 17 de septiembre de 2008 que señala que un número de teléfono móvil no es un dato personal si no puede asociarse a una persona identificada o identificable?

Las empresas que tienen páginas web y monitorizan las visitas tratando las IP's de sus usuarios: ¿cómo se recaban legalmente estos datos?, ¿basta un aviso legal en una página secundaria de la web?

- La AEPD, en aplicación de la LOPD, considerará la IP o el número de teléfono móvil como dato personal cuando pueda asociarse a una persona identificada o identificable (ver Dictamen 4/2007, de 20 de junio, del GT 29, sobre el concepto de dato personal. WP 136).

- **En la mayor parte de las ocasiones la legitimación para tratar las direcciones IP se basará, bien en el consentimiento informado (por ejemplo, usuarios registrados en la página web), bien en la relación jurídica en sentido amplio entre el titular de la web y el usuario de sus servicios (por ejemplo, usuarios no registrados de un buscador en Internet). En ambos casos el aviso legal puede no estar en la página principal siempre que sea identificable, fácilmente accesible y comprensible.**
- **Sin embargo deben tenerse en cuenta que tanto la LGT como la LSSI reconocen derechos y garantías específicos cuando se utiliza un número de móvil o se trata una dirección IP que son independientes del concepto de dato personal, siendo exigibles incluso cuando sus titulares son personas jurídicas.**

Cuando un médico utiliza el quirófano de un hospital privado para operar facilitándole el hospital servicios de anestesia y enfermería, entendemos que existen dos responsables de los datos distintos, ¿sería necesario el consentimiento del paciente para la cesión de sus datos por parte del médico con anterioridad a la operación para la reserva del quirófano y demás gestiones o estaría amparada en el artículo 11.2.c) LOPD?

- El tratamiento y cesión de datos de salud sólo puede ampararse en el consentimiento expreso del afectado o en una habilitación legal (art. 7.3 LOPD), y no en la existencia de una relación jurídica que implique necesariamente la conexión con ficheros a terceros.
- El tratamiento de los datos por parte del centro sanitario donde se va a realizar la intervención quirúrgica puede ampararse en el artículo 7.6 de LOPD (siempre que se realice para profesionales sanitarios sujetos al secreto profesional u otros con una obligación equivalente de secreto) y en el art.8 LOPD que legitima el tratamiento por las instituciones y centros sanitarios (públicos y privados) y los profesionales correspondientes, de los datos de las personas relativos a la salud que acudan a ellos o hayan de ser tratados en los mismos, de acuerdo con la legislación sanitaria.
- En el caso planteado, existirán dos responsables distintos.

¿Cómo debe recabar el consentimiento un autónomo para que sea válido en el caso de que en algún momento decida constituir una sociedad cuya actividad sea la misma y la finalidad del consentimiento también? ¿sería necesario recabar un nuevo consentimiento?

- **Cuando hay una modificación del responsable del fichero como consecuencia de una reestructuración societaria, manteniéndose la misma actividad y los datos se utilizan para la misma finalidad, no es necesario un nuevo consentimiento. En tal caso basta con informar a las personas afectadas de los extremos contemplados en el artículo 5 LOPD.**

¿Qué tipo de contrato o cláusula debería regular la relación contractual entre una empresa de trabajo temporal (ETT) y una empresa usuaria de sus servicios en relación a la LPOD?

- **La comunicación por la ETT de los datos de las personas vinculadas a ella al tercero usuario de sus servicios constituye una cesión que está legitimada por las relaciones jurídicas que la ETT mantiene con unos y otros.**
- **El tratamiento de los datos por parte de la tercera empresa, usuaria de los servicios de la ETT, se encuentra, también, legitimado por ser necesario para el mantenimiento o cumplimiento de dicha relación jurídica. Por tanto, no es necesario un contrato de prestación de servicios con la ETT como encargado del tratamiento.**

¿Qué obligaciones respecto a la protección de datos tenemos las organizaciones de formación que damos a nuestros alumnos accesos temporales a contenidos, informes, etc... a través de un campus virtual, así como lo que damos a los formadores/tutores de los mismos, incluyendo datos de los estudiantes?

- **El tratamiento de datos por los formadores/tutores estaría legitimado por la relación jurídica establecida con los alumnos.**
- **El acceso a contenidos debería excluir los datos personales a terceros, salvo que el mismo estuviera legitimado conforme a las reglas generales de la LOPD y el RLOPD.**

Guardar el resultado de un “macheo” de listas de clientes contra listas oficiales de terroristas, ¿va en contra de la LOPD? ¿Y guardar un listado de clientes sobre los que se solicita información por parte del juzgado para analizar operaciones sospechosas?

- **La normativa que regula la prevención y bloqueo de la financiación del terrorismo (Ley 12/2003, de 21 de mayo) y la prevención del blanqueo de capitales (Ley 19/1993, de 28 de diciembre) imponen a las personas y entidades obligadas que enumeran, a examinar cualquier operación que pueda estar relacionada con la financiación de actividades terroristas o vinculada al blanqueo de capitales.**
- **Entre las obligaciones que impone a los sujetos obligados está la de conservar durante un periodo mínimo de 6 años los documentos acreditativos de las comprobaciones que deban realizar (RD.925/1995, de 9 de junio).**

Por tanto, dicha conservación no va en contra de la LOPD al estar amparada legalmente en los dos casos planteados siempre que la información sea relevante para cumplir las obligaciones que le imponen las leyes citadas.

Corresponsabilidad de ficheros: En el ámbito de la educación y entre los Departamentos o Consejerías de Educación de las Comunidades Autónomas y los centros docentes públicos, ¿se puede entender que existe una corresponsabilidad del art. 57 RLOPD, respecto del fichero de alumnos?

- **No es posible admitir la corresponsabilidad del fichero de alumnos conforme al art.57 RLOPD dado que uno de los aspectos básicos de la creación y registro de ficheros es la finalidad y las relacionadas con las competencias de la Consejería y las funciones del colegio no son coincidentes, ya que las primeras son más amplias.**
- **Sin embargo, se puede atribuir la responsabilidad de los ficheros a la Consejería o al colegio público. En el caso de ser necesaria una comunicación de datos esta sería legítima en el marco de sus competencias y funciones.**
- **En el caso de los centros privados concertados debe diferenciarse entre el fichero de la Consejería y el centro de enseñanza, ya que el hecho de ser concertado no altera la responsabilidad de uno y otro. Cabrían, no obstante cesiones de datos entre ambos que fueran proporcionadas a sus competencias y responsabilidades, respectivamente**

En el caso de que contractualmente el responsable del fichero no informe al encargado del tratamiento de los tipos de datos que va a tratar y, por tanto, no informe sobre las medidas de seguridad que deben implantarse, ¿implica que el encargado del tratamiento se exime de las responsabilidades porque desconoce estos datos, o debe solicitar al responsable del fichero esa información hasta que la obtenga?

- **La implantación de las medidas de seguridad exigibles es una obligación tanto del responsable del fichero como del encargado del tratamiento (art.79 RLOPD)**
- **El responsable del fichero tiene una obligación específica de diligencia en orden a estipular en el contrato de prestación de servicios las medidas de seguridad que debe implantar el encargado del tratamiento (art.12 LOPD y 20.2 RLOPD). Por ello el encargado debe solicitar al responsable la indicación de las medidas.**

- **Si, pese a ello, no las estipula y el encargado del tratamiento puede conocer la tipología de datos objeto de la prestación de servicios deberá implantar las medidas de seguridad exigibles, sin perjuicio de la responsabilidad de quien lo contrató y no las indicó.**
- **Si el conocimiento de toda la tipología de datos objeto de la prestación de servicios fuera desproporcionado y el responsable no responde a sus requerimientos podría limitar o excluir la responsabilidad remitiendo al responsable una comunicación sobre el nivel de medidas de seguridad que va a implantar con la información de que dispone.**

En entidades de recobro, ¿qué uso se puede hacer de la información facilitada por el cliente, relativa al impagado que hayan obtenido otras entidades de recobro contratadas anteriormente? Si un cobrador va a la dirección de un moroso que aparece en páginas blancas, ¿puede tomar del buzón la escalera, piso y letra de la casa para remitir la carta?

- Con carácter general, las empresas de recobro desarrollan su actividad como encargadas del tratamiento debiendo limitarse a tratar los datos personales facilitados por el acreedor que les contrató.
- Para la obtención de datos adicionales han de estar legitimados conforme a la LOPD (consentimiento, habilitación legal, relación comercial...) siendo lo más habitual que obtengan datos de fuentes accesibles al público, como son las guías telefónicas.
- La obtención de datos adicionales no está, en principio, amparada en la prestación de servicios de recobro por lo que la empresa que los obtenga tendrá la condición de responsable de su tratamiento.

- **En tal condición las anteriores empresas de recobro sólo podrán ceder datos a las que intervengan posteriormente si tienen legitimación para la cesión que, probablemente, sólo existirá cuando se hayan obtenido de fuentes accesibles al público.**
- **En las guías telefónicas no consta, salvo consentimiento del afectado la escalera, piso y letra de la casa por lo que estos datos, al no figurar en una fuente accesible al público no pueden ser tratados sin consentimiento (u otra legitimación específica)**

Los clientes han cancelado todos los contratos con la entidad pero no han manifestado su negativa a recibir comunicaciones comerciales. No han manifestado su consentimiento expreso pero sí el tácito para recibir publicidad puesto que en otras ocasiones, cuando eran clientes, han sido llamados por teléfono y nunca se han opuesto. ¿Se les puede realizar una llamada telefónica no automática con intervención humana para intentar como clientes?

- La regla general, (en aplicación de la LOPD) si se tratan datos personales asociados al número de teléfono, es que sólo pueden recibir publicidad si se ha obtenido un consentimiento informado para ello o los datos se obtienen de fuentes accesibles al público.
- La mera realización de llamadas mientras eran clientes, sin que se hayan opuesto a ellas, es insuficiente para considerar que se ha obtenido el consentimiento.

- **Las llamadas no automáticas sin intervención humana (es decir, a través de una operadora), si están asociadas a datos personales, deben cumplir la regla general descrita, ya que se aplica la LOPD. Además, antes de realizarlas deberán consultarse los ficheros de exclusión que puedan existir (“listas Robinson”, art. 49 LOPD)**
- **Conforme al artículo 69.2 del RSU (RD 424/2005) tampoco se podrán realizar este tipo de llamadas, incluso si no están asociadas a datos de personas físicas (llamadas aleatorias) o afectan a personas jurídicas, respecto de aquellas que no figuran en guías telefónicas o que, figurando, aparezcan marcadas con el signo “U”, que significa que no quieren recibir publicidad. Al margen de estos casos, si no se tratan datos personales protegidos por la LOPD, pueden realizarse las llamadas pero los ciudadanos tienen la posibilidad de oponerse a ellas.**
- **Sin embargo, si se realizan, no podrán sancionarse al no existir un tipo de infracción específico para la vulneración de las garantías recogidas en el artículo 69.2 del RSU.**

¿El artículo 49 del RLOPD obliga al responsable del fichero a identificar de forma concreta cuáles son los ficheros comunes de exclusión, o bastaría con señalar que tales ficheros constan inscritos en la AEPD y que pueden consultarlos? ¿El artículo 49 se refiere al supuesto en el que los datos del afectado provengan de una fuente accesible al público?

- **El responsable del fichero ante el que el afectado manifiesta su negativa u oposición a que sus datos se traten con fines de publicidad o prospección comercial, deberá informar sobre los ficheros comunes de exclusión con indicación del responsable, su domicilio y la finalidad del tratamiento.**
- **No cabe, por tanto, la mera remisión al RGPD ya que dichos responsables pueden conocer la existencia de ficheros de exclusión, aunque no estén inscritos en el RGPD (por ejemplo, por haberlos constituido una asociación de la que forman parte).**
- **En todo caso, la información del RGPD, que es accesible a terceros, puede ser útil para cumplir la obligación del informar.**
- **La obligación de consultar previamente los ficheros de exclusión es exigible en los casos en que los datos personales figuren en fuentes accesibles al público.**

De acuerdo con el artículo 49 RLOPD, ¿es necesario consultar los Ficheros comunes de exclusión comercial para la realización de campañas de publicidad sobre clientes propios de un responsable de fichero frente al que no hayan ejercitado esos clientes el derecho de oposición?

- Si dispone de un consentimiento específico para realizar publicidad a los clientes, en principio, no habría que consultar.
- Sin embargo, si existen ficheros comunes de exclusión para las personas que no quieran recibir, en absoluto, ninguna publicidad, deberían consultarse estos ficheros.

Tengo una página web con un formulario de petición de datos y/o una base de datos de usuarios. La empresa española con la que contrato el mantenimiento y alojamiento de la página decide alojarla en un “hosting web” en EEUU ¿cómo regularizo la situación si la tercera empresa no está adherida a Acuerdo de Puerto Seguro? ¿Debo declarar una transferencia internacional? ¿Debo pedir el consentimiento a los afectados?

- El alojamiento en EEUU constituye una transferencia internacional de datos a un encargado del tratamiento en dicho país.
- El consentimiento informado de los afectados exime de la obligación de solicitar a la AEPD una autorización de transferencia internacional de datos.
- Si no se ha obtenido el consentimiento es preciso que el responsable titular de la página web solicite autorización para la transferencia internacional, que puede obtenerse suscribiendo las cláusulas contractuales tipo previstas en la Decisión de la Comisión Europea, 2002/16/CE de 27 de Diciembre de 2001.
- Las cláusulas contractuales deben ser suscritas por el responsable, el encargado del tratamiento en España y la tercera empresa que presta sus servicios en EEUU.

Se ha obtenido una autorización para realizar una transferencia internacional de varios ficheros y para una serie de datos. Si posteriormente se decide suprimir esos ficheros por realizar una reorganización interna de los mismos e inscribirse un nuevo fichero que refunda los antiguos ¿cómo comunicar a la AEPD para que la autorización de transferencia internacional tenga efectos para el nuevo fichero?

- No puede darse una respuesta unívoca de carácter general pues depende de los términos de refundición de los ficheros, los sujetos intervinientes en la transferencia y las condiciones de la autorización.
- No obstante, cabe la posibilidad de admitirla. Por ejemplo: Un operador de telecomunicaciones pasa a ser responsable de los ficheros de clientes que ha adquirido de otros dos operadores como consecuencia de una operación de reestructuración societaria. Cada uno de ellos tenía autorizadas las TID a un encargado del tratamiento en países distintos. El operador quiere refundir los ficheros de clientes con un solo encargado de los preexistentes. Podría modificar un fichero de clientes incorporando los restantes y conservar la autorización de TID.

Respecto de los documentos en soporte papel. ¿ Es necesario inventariar todos los documentos con datos de carácter personal que tenga el responsable del fichero o basta con inventariar los expedientes o carpetas en las que se encuentren archivados los documentos?

- **Respecto de los ficheros no automatizados el RLOPD exige (art. 92 y 106):**
 - La identificación del tipo de información de los documentos.
 - Su inventario.
 - El archivo (que puede estar regulado o ser definido por el responsable) conforme a criterios que garanticen la conservación, localización y consulta, así como que posibiliten el ejercicio de derechos.

Estas obligaciones deben ponerse en relación con el tipo y finalidad del sistema de información y de los ficheros existentes.
- **Así, por ejemplo, en un registro de entrada y salida deberá inventariarse cada documento como unidad diferenciada (una solicitud de empleo y el currículum anexo sería un documento).**
- **Pero en un fichero de expedientes o procedimientos el inventario puede hacerse por carpetas o expedientes en los que se archivan los documentos (por ejemplo el expediente laboral de un empleado, o la historia clínica de un paciente).**

En el caso de una federación cuya finalidad es el asesoramiento a entidades que trabajan con personas discapacitadas para la consecución de ayudas o programas diseñados por la Administración Pública (Estatal, Autonómica o Local), en ocasiones, para la tramitación de las ayudas deben solicitarse y aportarse los certificados de discapacidad de los solicitantes. ¿El certificado estaría incluido en la excepción del artículo 81.6 del RLOPD (medidas de seguridad de nivel básico)?

- El tratamiento del certificado de discapacidad, si se limita a incluir el grado de discapacidad o la declaración de la misma o de la invalidez, para la obtención de las ayudas citadas, puede considerarse como realizado “con motivo del cumplimiento de deberes públicos”, siendo exigible la implantación de medidas de seguridad de nivel básico.

La herramienta de trabajo de los medios de comunicación es la información ¿Qué medidas de seguridad han de implantar los medios de comunicación audiovisuales para cumplir la LOPD?

- **El nivel de seguridad (básico, medio o alto) depende de la naturaleza de los datos que se traten conforme al artículo 81 del RLOPD.**
- **Los medios de comunicación (audiovisuales o no) tratan con frecuencia informaciones relacionadas con la ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual de las personas, en cuyo caso sería exigible implantar, además de las medidas de seguridad de nivel básico y medio, las de nivel alto.**



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

