DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 4| Octubre 2020

LAS DIEZ INFRACCIONES MÁS HABITUALES EN PROTECCIÓN DE DATOS EN LAS ENTIDADES LOCALES

DIPUTACIÓ DE VALÈNCIA
Protecció de Dades i Seguretat de la Informació

ÍNDICE

LAS DIEZ INFRACCIONES MÁS HABITUALES EN PROTECCIÓN DE DATOS EN LAS ENTIDADES LOCALES

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

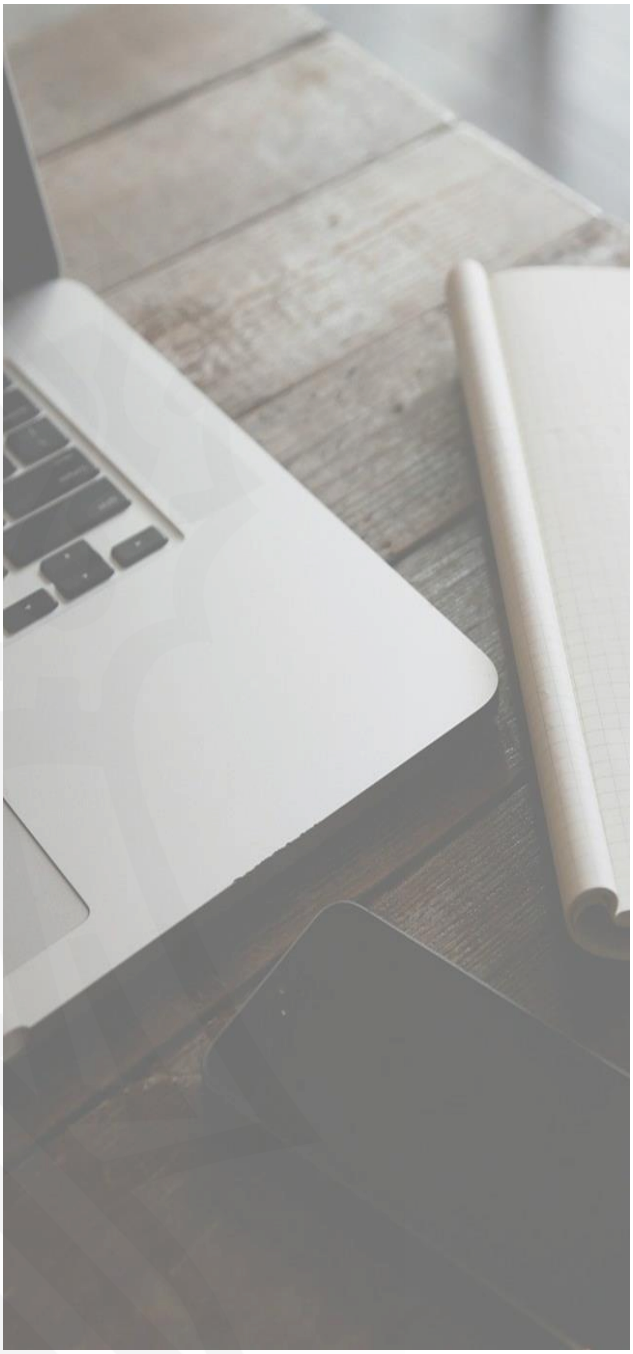
Pl. de Manises, 4 46003 Valencia

email: dpdssi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

LAS DIEZ INFRACCIONES MÁS HABITUALES EN PROTECCIÓN DE DATOS EN LAS ENTIDADES LOCALES



Una de las novedades que trajo consigo el Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) fue el endurecimiento del régimen sancionador, que incrementó notablemente la cuantía de las sanciones por el incumplimiento de lo previsto en la normativa de protección de datos.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) desarrolló el sistema de sanciones del RGPD, categorizando las **infracciones** en **muy graves, graves y leves**. Algunos de los actos sancionables de cada uno de los tres niveles son:

INFRACCIONES CONSIDERADAS MUY GRAVES

- Vulneración de **principios y garantías.**
- Tratamiento de datos sin **base de licitud.**
- Incumplimiento de los requisitos exigidos para la **validez del consentimiento.**
- Utilización de datos para **finalidades incompatibles** con la de recogida.
- Tratamiento de **categorías especiales** de datos sin que concurra una de las circunstancias previstas.
- Tratamiento de datos relativos a **condenas e infracciones penales o medidas de seguridad conexas**, o **infracciones y sanciones administrativas** fuer de los supuestos permitidos.
- La **omisión del deber de informar** al afectado acerca del tratamiento de sus datos.
- La vulneración del **deber de confidencialidad**.
- El **impedimento o la obstaculización o la no atención reiterada del ejercicio de derechos**.
- La **transferencia internacional de datos** sin concurrir garantías, requisitos o excepciones.
- El incumplimiento de la **obligación de bloqueo** de los datos.

INFRACCIONES CONSIDERADAS GRAVES

- El tratamiento de datos personales de un **menor de edad sin recabar su consentimiento**, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela.
- La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de **protección de datos desde el diseño.**
- La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, **por defecto**, solo se tratarán los **datos personales necesarios** para cada uno de los fines específicos del tratamiento.
- La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un **nivel de seguridad adecuado al riesgo** del tratamiento.
- La contratación por el responsable del tratamiento de **un encargado de tratamiento que no ofrezca las garantías suficientes**.
- Encargar el **tratamiento de datos a un tercero sin la previa formalización de un contrato** u otro acto jurídico en los términos del RGPD.
- No disponer del **registro de actividades de tratamiento**.
- El incumplimiento de la **obligación de designar un delegado de protección de datos** cuando sea exigible su nombramiento

INFRACCIONES CONSIDERADAS LEVES

- El incumplimiento del **principio de transparencia** de la información o el derecho de información del afectado por **no facilitar toda la información exigida**.
- **No atender las solicitudes de ejercicio de los derechos**.
- Disponer de un **registro de actividades de tratamiento que no incorpore toda la información exigida**.
- La **notificación incompleta, tardía o defectuosa a la autoridad** de protección de datos de la información relacionada con una **violación de seguridad** de los datos personales.
- El incumplimiento de la obligación de **documentar cualquier violación de seguridad**.
- El incumplimiento del **deber de comunicación al afectado de una violación de la seguridad** de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados.
- **No publicar los datos de contacto del delegado de protección de datos**, o **no comunicarlos a la autoridad de protección de datos.**

En el ámbito de la Administración Pública, el RGPD permite a los Estados establecer sus propias normas para regular el régimen sancionador de las mismas. En el caso de España, la LOPDGDD contempla para estas la sanción de **apercibimiento**, acompañada de las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción. Asimismo, ha de tenerse en cuenta el **daño reputacional** que la sanción causaría a la entidad

"EL RÉGIMEN SANCIONADOR APLICABLE A LAS ADMINISTRACIONES PÚBLICAS CONTEMPLA PARA ESTAS LA SANCIÓN DE APERCIBIMIENTO, QUE IRÁ ACOMPAÑADA DE LAS MEDIDAS QUE PROCEDA ADOPTAR PARA QUE CESE LA CONDUCTA O SE CORRIJAN LOS EFECTOS DE LA INFRACCIÓN. ASIMISMO, HA DE TENERSE EN CUENTA EL DAÑO REPUTACIONAL QUE LA SANCIÓN CAUSARÍA A LA ENTIDAD"

A continuación, haremos un repaso a las infracciones más habituales en protección de datos en las Entidades Locales:

EJERCICIO DE DERECHOS

El derecho fundamental a la protección de datos reconoce a los interesados la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos. Entre los derechos que la Ley otorga a los interesados en relación con sus datos personales están los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento, portabilidad de los datos y a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos.

Las solicitudes deben ser siempre atendidas sin demora y en el plazo máximo de un mes. Si el Responsable del Tratamiento no da curso a la solicitud del interesado, le debe informar sin demora injustificada, y a más tardar al mes de la recepción de la solicitud, de las razones por las que no ha actuado, así como de la posibilidad de presentar una reclamación ante una autoridad de control y recurrir a los tribunales.

Éste constituye uno de los aspectos más importantes de la legislación relativa a la protección de datos de carácter personal, dado que un mal conocimiento o mala gestión del procedimiento de ejercicio de derechos suele ser la antesala de un procedimiento sancionador.

De hecho, la indebida atención a las solicitudes de los ciudadanos en el ejercicio de los derechos que establece el RGPD es, en la práctica, una de las infracciones más habituales en el ámbito de las Entidades Locales. En especial, destaca la indebida atención de los derechos de acceso y supresión, seguidos por el derecho de oposición y el de rectificación.

En la Resolución nº R/00171/2020, la Agencia Española de Protección de Datos (AEPD) sancionó a una Entidad Local por no haber sido debidamente atendido un derecho de supresión. En concreto, el reclamante solicitó la eliminación de sus datos personales de en enlace de la web municipal. Si bien la Entidad Local reclamada mostró su voluntad de atender el derecho, no lo hizo efectivo.

En la Resolución nº R/00180/2020 de la AEPD, por su parte, la Entidad Local fue sancionada por no dar la respuesta legalmente exigible a la solicitud de supresión ejercida por el reclamante.

VIDEOVIGILANCIA

La imagen de una persona, en la medida que identifique o pueda identificar a la misma, constituye un dato de carácter personal que puede ser objeto de tratamiento para diversas finalidades, siendo común la de garantizar la seguridad de personas, bienes e instalaciones municipales.

Estos tratamientos de datos habrán de cumplir con lo dispuesto en el art. 22 LOPDGDD, que dispone entre otras cosas, que los tratamientos de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, el deber de información puede cumplirse mediante la colocación, en las zonas videovigiladas, de un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados, y sirviéndose de impresos en los que se detalle la información prevista, que el responsable deberá poner a disposición de los interesados.

Por otra parte, solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Son numerosas las sanciones que impone la AEPD por no cumplir con las previsiones del art. 22 LOPDGDD.

En el Procedimiento Nº: PS/00384/2019, si bien las imágenes de las cámaras que instala la Entidad Local se limitan a la zona de acceso a las instalaciones, considerándose las mismas proporcionadas con la finalidad de control de acceso a unas instalaciones deportivas, se sanciona a la entidad porque el sistema no disponía inicialmente de cartel informativo, ni de formulario informativo adaptado a la normativa en vigor.

DEBER DE INFORMACIÓN

El art. 13, apartados 1 y 2, del RGPD, establece la información que debe facilitarse al interesado en el momento de la recogida de sus datos: identidad y datos de contacto del responsable, datos de contacto del Delegado de Protección de Datos (DPD), fines del tratamiento, base jurídica, destinatarios, intención de realizar transferencias internacionales, plazo de conservación, existencia de derechos, derecho a presentar una reclamación ante la autoridad de control, etc.

No obstante, las Entidades Locales no siempre la facilitan o lo hacen de forma incompleta, lo que constituye una infracción en materia de protección de datos.

En el Procedimiento nº PS/00347/2019, se sanciona a una Entidad Local por vulneración del art. 13 del RGPD, respecto de la falta de información que se proporcionó a los trabajadores y funcionarios del Ayuntamiento cuando se obtuvieron sus datos personales para la elaboración de la relación de puestos de trabajo (RPT).

OBTENCIÓN DEL CONSENTIMIENTO

En relación con el consentimiento para tratar datos de carácter personal, el legislador europeo ha concebido este como una causa más de licitud o legitimación para realizar el tratamiento de datos. Ahora bien, el consentimiento ha de cumplir con las condiciones requeridas por el RGPD. Entre estas condiciones, se encuentra la del art. 7.2 RGPD que establece que, si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se debe presentar de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

Sin embargo, ante la ausencia de otra base en la que legitimar el tratamiento de los datos, las Entidades Locales no siempre solicitan el consentimiento, u obtienen un consentimiento que no cumple con las condiciones exigidas por el RGPD.

En la Resolución R/03041/2017, la AEPD sancionó a una Entidad Local por crear un grupo de WhatsApp en el que incorporó 255 números de teléfono de vecinos del municipio para facilitar la comunicación con estos, ello a pesar de que estos no habían otorgado su consentimiento para dicho tratamiento.

Por su parte, en el Procedimiento PS/00382/2019, si bien la Entidad Local reclamada solicitó el consentimiento para la participación en actividades lúdicas organizadas por el municipio para menores y la publicación de imágenes de estos, fue sancionada por obtener el consentimiento para todas las actividades en general, debiendo recogerse para cada una de ellas.

PUBLICACIÓN DE LAS ACTAS DE LA JUNTA DEL GOBIERNO LOCAL

La Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local establece en su artículo 70.1 que las sesiones del Pleno de las Corporaciones Locales son públicas, salvo en aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución, cuando así se acuerde por mayoría absoluta y también, que las sesiones de la Junta de Gobierno Local no son públicas. Por otra parte, el apartado 2 del referido artículo 70 establece que los acuerdos que adopten las corporaciones locales se publicarán o notificarán en la forma prevista por ley.

El artículo 88.1 del R.D. 2568/1986, de 28 de noviembre, del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, establece el carácter público de las sesiones del Pleno, con la posibilidad de celebrar a puerta cerrada el debate y votación de aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18 de la Constitución, cuando así se acuerde por mayoría absoluta. A su vez, el artículo 229 del RD 2568/1986 establece que las Corporaciones darán publicidad resumida del contenido de las sesiones plenarias y de todos los acuerdos del Pleno y de las Comisiones de Gobierno, así como de las resoluciones del Alcalde.

La conclusión es que las Entidades Locales pueden publicar de forma resumida el contenido de las sesiones y acuerdos del Pleno y las Comisiones, pero sin incluir más datos de los que sean adecuados, pertinentes y no excesivos en relación con la finalidad pretendida, lo que no siempre cumplen las Entidades Locales, publicando el contenido íntegro de las Actas de la Junta de Gobierno Local.

En la Resolución R/00387/2018, la AEPD sancionó a una Entidad Local por publicar en su página web el contenido íntegro del Acta de la Sesión Ordinaria celebrada por la Junta de Gobierno Local, en la que se hacía referencia a una solicitud de devolución de una donación realizada por la reclamante, lo que supone una indebida divulgación de sus datos de carácter personal.

PUBLICACIÓN DE DATOS PERSONALES EN PROCESOS SELECTIVOS

En los procedimientos selectivos, el principio de publicidad y transparencia se torna en esencial, como garantizador del principio de igualdad, aunque para asegurar el cumplimiento del principio de publicidad la Ley no especifica ningún medio concreto, pudiendo existir casos en los que la forma de publicación por la que se ha optado pueda considerarse excesiva. La proporcionalidad y adecuación del tratamiento han de estar conformes con el principio de transparencia para los participantes en el proceso, y no resulta necesario para ello exponer los datos en abierto para cualquier persona no participante en el proceso. Un modo satisfactorio de cumplir el objetivo sería prever un sistema en el que todos los participantes puedan acceder a la información, puesto que se trata de concurrencia competitiva, pero dicha información no debe ser accesible a terceros no participantes en el proceso, afectando la trasparencia exclusivamente a los admitidos o excluidos. Por tanto, ni el turno por el que se presentan los candidatos ni el nombre y apellidos en el puesto al que optan es necesario que sea accesible por personas que no participan en el proceso.

No obstante, no en pocas ocasiones nos encontramos con que las Entidades Locales hacen públicas, en abierto, en sus páginas webs o incluso en sus Redes Sociales, las listas de admitidos y excluidos en procedimientos de concurrencia competitiva, lo que conlleva la imposición de sanciones por parte de las autoridades de control.

En el Procedimiento nº AP/00046/2018, la AEPD sancionó a una Entidad Local por publicar en su página web y en sus redes sociales la lista del personal seleccionado en el marco de un Plan de Cooperación Local, incluidos el nombre y apellidos de los aspirantes ligados a su condición de discapacitado.

CORREOS ELECTRÓNICOS SIN COPIA OCULTA

El envío de correos electrónicos debe atender también las obligaciones recogidas en la normativa vigente de protección de datos, en particular en lo relativo a preservar la confidencialidad y datos personales concernientes a los destinatarios de los mensajes. A este respecto, se considera preciso el recurso a una modalidad de envío que ofrecen los programas de correo electrónico disponibles en el mercado, la cual permite detallar las direcciones electrónicas de los destinatarios múltiples en un campo específico del encabezado del mensaje: el campo CCO (con copia oculta), en lugar del habitual CC.

En la Resolución R/01625/2018, la AEPD sancionó a una Entidad Local por remitir a 12 destinatarios el listado final del curso de "Operaciones auxiliares de montaje de redes eléctricas", con las direcciones de correo electrónico de todos los destinatarios visibles para todos ellos.

PUBLICACIÓN DE RESOLUCIONES JUDICIALES

El principio de publicidad de las actuaciones judiciales se encuentra consagrado, en cuanto a las sentencias, por los artículos 205.6, 232, 235, 235 bis, 235 ter y 266 de la Ley Orgánica del Poder Judicial. La publicidad a la que se refieren dichos preceptos tiene por objeto asegurar el pleno desenvolvimiento del derecho de las partes a obtener la tutela efectiva de los jueces y Tribunales en el ejercicio de sus derechos, sin que en ningún modo pueda producírseles indefensión, consagrado por el artículo 24.1 de la Constitución. La colisión entre la publicidad de las sentencias y el derecho a la intimidad de las personas ya ha sido analizada por la AEPD, que en base a lo dispuesto por el Consejo General del Poder Judicial, ha entendido que en el tratamiento y difusión de las resoluciones judiciales se debe procurar la supresión de los datos de identificación para asegurar en todo momento la protección del honor e intimidad personal y familiar.

Es por ello que, las resoluciones judiciales de los procedimientos en los que las Entidades Locales sean parte no pueden ser difundidas íntegramente en Tablones en las dependencias de la entidad, ni en su página web.

En la Resolución nº R/00036/2018 se sancionó a una Entidad Local por colocar una nota informativa con todos los datos de la sentencia judicial en la que se condenaba a un vecino en un pleito contra el Ayuntamiento, en tres tablones de anuncios del municipio, y en la página de Facebook de la localidad.

SEGURIDAD DEL TRATAMIENTO Y NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, las Entidades Locales deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos. Además, en caso de violación de la seguridad de los datos personales, deben notificar a la autoridad de control competente sin dilación indebida y, a más tardar, 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Asimismo, cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, la Entidad Local lo deberá comunicar también al interesado sin dilación indebida.

No obstante, las Entidades Locales no siempre aplican las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo y, en caso de incidente de seguridad, no siempre lo gestionan correctamente.

En el Procedimiento nº PS/00463/2019, la AEPD sanciona a una Entidad local por mostrar en su Sede Electrónica 23 certificados de diversa índole relacionados con el padrón donde aparecen datos personales de los componentes de la familia del reclamante y de los interesados de otros 22 certificados firmados el mismo día, pues todos los certificados firmados el mismo día tenían el mismo CSV. Además, tampoco dio cumplimiento a la obligación de notificarlo a la autoridad de control, así como a los posibles afectados por el incidente sin dilaciones indebidas una vez tuvo el conocimiento de ello.

NOMBRAMIENTO DEL DELEGADO DE PROTECCIÓN DE DATOS

En el marco del RGPD la figura del DPD ha emergido gracias, principalmente, a su exigibilidad en diferentes supuestos; y también gracias a que es una de las medidas que componen uno de los principales principios del RGPD: la responsabilidad activa.

Uno de los supuestos de obligada designación se da cuando el tratamiento lo lleve a cabo una autoridad u organismo público, lo que implica que todas las Entidades Locales tengan que designar un DPD.

Si bien no es una de las infracciones más habituales en el ámbito local, es una conducta que la AEPD empieza a sancionar.

En el Procedimiento PS/00001/2020, la AEPD sancionó a una Entidad Local por carecer de Delegado de Protección de Datos.

MATERIAL COMPLEMENTARIO

- Resolución AEPD Nº: R/00171/2020 (ejercicio de derechos)
- Resolución AEPD Nº: R/00180/2020 (ejercicio de derechos)
- Resolución AEPD Procedimiento Nº: PS/00384/2019 (videovigilancia)
- Resolución AEPD Procedimiento Nº: PS/00347/2019 (deber de información)
- Resolución AEPD Procedimiento Nº AP/00023/2017 (consentimiento)
- Resolución AEPD Procedimiento Nº: PS/00382/2019 (consentimiento)
- Resolución AEPD Nº R/00387/2018 (Actas Junta de Gobierno Local)
- Resolución AEPD Procedimiento Nº AP/00046/2018 (Procedimientos selectivos)
- Resolución AEPD Procedimiento Nº AP/00037/2017 (copia oculta)
- Resolución AEPD Procedimiento Nº: PS/00463/2019 (publicación de resoluciones judiciales)
- Resolución AEPD Procedimiento Nº: PS/00001/2020 (DPD)

NOTICIAS

- **Se publica el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.** En su capítulo IV, el Real Decreto-Ley se refiere de manera específica a las facultades de organización, dirección y control empresarial en el trabajo a distancia, incluyendo la protección de datos y seguridad de la información, el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales y las instrucciones necesarias para preservar a la empresa frente a posibles brechas de seguridad. Consulta la norma en este enlace.

- **Se publica la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.** Esta incluye una serie de disposiciones en materia de protección de datos, entre las que figuran la obligación de conservación de la documentación relativa a los sistemas y procedimientos de tratamiento; la obligación de registro de las operaciones de recogida, consulta, transferencia y supresión de los datos, así como la obligación de comunicar al interesado y a la autoridad nacional de control cualquier violación de los datos personales que dé lugar a un elevado riesgo para la protección de los mismos o afecte negativamente a la intimidad del interesado. Consulta la norma en este enlace.

- **La AEPD publica recomendaciones para minimizar los riesgos para la privacidad en la navegación por Internet**. La nota repasa algunas de las técnicas más utilizadas por páginas web y servicios de internet para hacer seguimiento de los sitios web que visitan los usuarios. La Agencia incluye un apartado de recomendaciones básicas dirigidas a usuarios con un nivel de conocimientos medio, como la importancia de valorar la privacidad como una característica deseable al elegir un navegador y las aplicaciones que se instalen; evitar la instalación de aplicaciones innecesarias en el navegador; activar, en su caso, la protección anti-rastreo o seguimiento en el navegador, o configurarlo para bloquear las cookies de terceros, o al menos bloquearlas si se navega en modo privado, entre otras. Asimismo, recoge recomendaciones para usuarios avanzados. Consulta la Nota en este enlace.