GARRIGUES

Newsletter Economía del Dato, Privacidad y Ciberseguridad

Noviembre de 2025

Índice

1. ¿El dato personal seudonimizado es un dato personal? Claves tras la sentencia del Tribunal de Justicia de la UE en el asunto EDPS v SRB
2. Comparativa de la transposición de la NIS II por parte de Portugal con la prevista en España
3. Resoluciones de las autoridades de protección de datos
4. Sentencias
5. Actualidad

1. ¿El dato personal seudonimizado es un dato personal? Claves tras la sentencia del Tribunal de Justicia de la UE en el asunto *EDPS v SRB*

La sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del pasado 4 de septiembre de 2025 en el caso EDPS v SRB (asunto C 413/23 P) supone un hito importante en el campo de la protección de datos personales, al tratar un tema tan esencial para la práctica como el mismo concepto de "dato personal".

Ignacio Suárez

En este asunto fueron parte el Supervisor Europeo de Protección de Datos (SEPD o *EDPS* por sus siglas en inglés) y la Junta Única de Resolución (JUR o *SRB* por sus siglas en inglés). El litigio trae causa de la resolución de Banco Popular (que tuvo lugar mediante decisiones de la JUR y el FROB en España de 7 de junio de 2017) y del procedimiento de "derecho de audiencia" abierto por la JUR en 2018 para evaluar una eventual compensación a accionistas y acreedores, en el que se recabaron datos y comentarios mediante un registro y un formulario en línea. Los comentarios sobre la "valoración 3" (1.104 en total) fueron transmitidos el 17 de junio de 2019 por la JUR a Deloitte a través de un servidor virtual seguro. A raíz de varias reclamaciones, el SEPD apreció en 2020 que la JUR no había informado a los interesados de que Deloitte podía ser destinataria de esos datos en la declaración de confidencialidad del procedimiento, decisión (luego revisada) que la JUR impugnó y que desembocó en la sentencia del TJUE de 4 de septiembre de 2025.

El tema de mayor calado discutido en este caso, y que viene generando un intenso e interesante debate entre los profesionales del sector, es si un dato seudónimo o seudonimizado es en sí mismo un dato personal por defecto (al no estar entera e irrevocablemente anonimizado), o si puede ser un dato "no personal" para quien no pueda, sin esfuerzos desproporcionados, vincular ese dato a una persona física.

Podría pensarse que algo tan elemental no debería ser objeto de debate a estas alturas, pero lo cierto es que la redacción de la normativa ha dado pie a diferentes perspectivas sobre lo que debe considerarse, o no, como dato personal. Así, se han venido fraguando dos visiones diferentes sobre este concepto:

- **La doctrina absoluta:** que considera como dato personal cualquier información que, de manera directa o indirecta, pudiera asociarse a una persona física, por remota o improbable que pudiera ser esta vinculación.

- **La doctrina subjetiva**: que considera que un dato solo será personal para quien tenga medios razonables para vincular este dato a un individuo.

De este modo, se aprecia que una aplicación estricta de la teoría absoluta conduce a la conclusión de que un dato es o personal o no personal en sí mismo, con independencia de quién lo tenga en su poder. Así, por ejemplo, un código seudonimizado sería un dato personal para un sujeto, aunque este fuera incapaz de vincularlo con una persona física, siempre que, en algún lugar, algún responsable tuviera la "llave" o tabla de correspondencia que permitiera esta reidentificación.

Esta interpretación "monolítica" del concepto de dato personal, si bien trata de ser especialmente garantista con los derechos de los interesados, resulta en cargas regulatorias en ocasiones inasumibles para los responsables del tratamiento. Sin perjuicio de ello, durante mucho tiempo ha venido siendo la interpretación seguida mayoritariamente por las autoridades de supervisión en materia de protección de datos y, en consecuencia, por los operadores, por conllevar un menor riesgo de incumplimiento normativo para los responsables del tratamiento.

No obstante, en los últimos tiempos esta concepción ha venido siendo rebatida en sentencias del TJUE, como en los casos *Breyer* y *Scania*. En estas sentencias, el Tribunal se decanta por la doctrina subjetiva, al indicar, en resumidas cuentas, que una dirección de IP dinámica (en *Breyer*) o un número de identificación de vehículo (VIN) (en *Scania*) son datos personales solo en tanto en cuanto una entidad pueda vincular esa información con una persona física.

Si bien cabría esperar que, con el aval de las citadas sentencias del TJUE, la posición subjetiva estaría totalmente asentada y aceptada, restando así importancia a la resolución que nos ocupa, no es el caso. Ciertas autoridades, como el mismo Comité Europeo de Protección de Datos en sus recientes Directrices 1/2025 sobre el concepto de seudonimización -solo disponibles, actualmente, en su versión preliminar de consulta pública-, siguen adoptando un criterio ciertamente restrictivo, más tendente a la doctrina absoluta que a la subjetiva.

Es por ello que la resolución del TJUE objeto de este comentario es de gran calado, pues no solo se reafirma en la doctrina subjetiva, sino que, además, declara por vez primera de manera meridianamente clara que un dato personal seudonimizado (en este caso, un código alfanumérico relativo a una persona) tratado por un responsable "A" puede ser un dato personal para "A" y no serlo para un cesionario "B" en caso de que este no pueda (razonablemente) llevar a cabo una vinculación o reidentificación del dato.

Esto no solo supone una revalidación de la doctrina subjetiva, sino que tiene importantes implicaciones prácticas que se detallan a continuación.

Implicaciones prácticas

Dado que para el responsable "A" el dato seudonimizado será, en todo caso, un dato personal (al tener la capacidad de reidentificar al interesado a partir del código alfanumérico), "A" debería cumplir a todos los efectos con la normativa aplicable. Ello implica que, entre otras obligaciones, deberá:

- contar con una base legal (art. 6 RGPD) para llevar a cabo el tratamiento de ese dato personal, incluyendo, en su caso, una base legal suficiente para su cesión a un tercero; e

- informar del tratamiento al interesado, en cumplimiento de los arts. 13 o 14 del RGPD, según proceda, incluyendo información sobre las cesiones a destinatarios que fueran a recibir sus datos personales. En este sentido, se pronuncia el TJUE en la resolución de referencia, aunque por los detalles del caso, cabe cierto margen de interpretación sobre qué clase de información se debería facilitar a interesados sobre cesionarios que no vayan a poder llevar a cabo la vinculación de los datos pseudónimos con los interesados.

En relación con el cesionario "B", este podría ser considerado responsable del tratamiento a todos los efectos si puede razonablemente reidentificar al interesado. No obstante, en caso de que el cesionario "B" no sea considerado, en aplicación de la doctrina subjetiva, responsable del tratamiento (al no estar tratando, desde su punto de vista, datos personales), surgen preguntas de difícil respuesta como las siguientes:

¿Qué derechos tiene el interesado ante el cesionario de los datos?

La resolución de referencia apunta a que el interesado podrá ejercer sus derechos de protección de datos tanto frente al cedente como al cesionario. Para este último, sin embargo, podría resultar materialmente imposible dar respuesta, por ejemplo, a ejercicios de derecho de acceso o supresión, dado que la información no sería personal a sus efectos.

¿Qué información debe facilitar entonces el cedente a los interesados en relación con cesionarios que no puedan identificar al interesado?

Con ánimo de racionalizar las exigencias informativas de los responsables cedentes y evitar situaciones de confusión entre los interesados y los cesionarios que no les puedan identificar, se podría plantear la posibilidad de que los cedentes: (i) informen únicamente de las categorías de cesionarios para los cuales la información recibida no será información personal (sin identificar uno a uno a los cesionarios); o (ii) informen de que determinados cesionarios no podrán identificarles con la información recibida, anticipándose así a las problemáticas identificadas. Como se indicaba anteriormente, en este punto la resolución del TJUE deja cierto margen de apreciación (a la vista, por ejemplo, de las bases legales que apliquen en cada caso).

¿Aplica esto a los encargados del tratamiento?

Para el caso de relaciones de encargado del tratamiento, surgen importantes dudas sobre el encaje de esta doctrina en casos en los que la entidad "encargada" opere siguiendo las instrucciones del responsable, pero tratando datos seudónimos que no supongan, para el encargado, información personal. En este caso, la prudencia invita a entender que no sería de aplicación la teoría subjetiva en su totalidad, pues, al estar operando por cuenta del responsable, sería difícil argumentar que el encargado está tratando datos "no personales" (al seguir las instrucciones del responsable, las posibilidades de reidentificación no deben entenderse como remotas en caso alguno). No obstante, este es un caso a estudiar en mayor detalle, pues las implicaciones prácticas de aceptar la plena aplicabilidad de la doctrina subjetiva a estos efectos serían mayúsculas (piénsese en las facilidades que implicaría a la contratación con terceros).

Conclusiones

La sentencia del TJUE en el caso de *EDPS v SRB* supone no solo una revalidación de la ya conocida doctrina subjetiva, sino también un importante hito a tener en cuenta por los profesionales de la práctica, al dar muy relevantes perspectivas sobre la implementación de esta doctrina. En particular:

- Aclara que un dato seudónimo puede ser, o no, un dato personal, dependiendo de quién lo trate y las posibilidades reales de identificación de personas físicas, y da apuntes sobre las obligaciones de cedentes y cesionarios de datos seudonimizados, que deberán ser estudiadas en detalle para su correcta adopción.

- Abre un nuevo terreno a explorar por los profesionales de la protección de datos, que deberán tener sus conclusiones en cuenta a la hora de estructurar los esquemas de cumplimiento normativo de responsables y encargados. Por ejemplo, sus implicaciones en lo relativo al uso de información seudonimizada para entrenamientos de modelos de IA puede ser de gran interés

para los tenedores de grandes volúmenes de información personal, pues podría facilitar su comercialización.

- Esta sentencia exige una nueva perspectiva no solo de cara a las nuevas cesiones o encargos a regularizar, sino también un replanteamiento de las estructuras ya establecidas, que podrían verse afectadas por esta interpretación de la normativa.

2. Comparativa de la transposición de la NIS II por parte de Portugal con la prevista en España

En julio de 2025, el Gobierno portugués reanudó el proceso de transposición de la Directiva (UE) 2022/2555 (NIS II) mediante la presentación del Proyecto de Ley n.º 7/XVII/1. En este análisis, comparamos dicha transposición con el proyecto de ley español, examinando los ámbitos de aplicación sujetos y exentos en cada caso, así como el régimen sancionador previsto.

Manuel Liberal Jerónimo y **Luisa Cyrne**

El anterior proyecto de ley de Portugal (Proyecto de ley Nº 50/XVI/1) expiró con la disolución de la Asamblea de la República, el 11 de marzo. Actualmente, Portugal sigue incumpliendo el plazo de transposición de octubre de 2024, que llevó a la apertura del procedimiento de infracción por parte de la Comisión Europea en noviembre del mismo año.

En comparación con el proyecto de ley español (Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad), una de las principales diferencias está relacionada con el ámbito de aplicación:

Ámbito sujeto de aplicación

Portugal	España
Entidades privadas	**Entidades públicas o privadas**
▪ **De los sectores críticos:** Energía; transporte; banca; infraestructura del mercado financiero; salud; agua; infraestructura digital[1]; proveedores de servicios administrados; y espacio.	

[1] Esto incluye a los proveedores de puntos de intercambio de internet, de servicios de DNS, los registros de nombres de los TLD, los proveedores de servicios de computación en nube, de servicios de centros de datos, I de redes de distribución de contenidos, de servicios de confianza, de redes públicas de comunicaciones electrónicas y de servicios de comunicaciones electrónicas disponibles al público.

Portugal	España
▪ **De otros sectores críticos:** Servicios postales y de mensajería; gestión de residuos, producción, fabricación y distribución de productos químicos; producción, fabricación y distribución de productos alimenticios; fabricación; prestación de servicios digitales[2]; investigación. **España también añade: la industria nuclear y los sectores de la seguridad privada.**	
▪ Administración pública. ▪ Oficina del Defensor del Pueblo. ▪ Consejo Económico y Social. ▪ Servicios técnicos y administrativos de la Presidencia de la República, la Asamblea de la República, los Tribunales, el Consejo Superior de la Judicatura, el Consejo Superior de los Tribunales Administrativos y Tributarios y el Consejo Superior del Ministerio Público.	▪ Entidades de la administración pública, excluidos el poder judicial, los parlamentos y los bancos centrales.
▪ Instituciones de educación superior.	▪ Universidades y centros de investigación (en asuntos o proyectos de investigación relacionados con sectores críticos)
Entidades críticas (por designar)	

Exclusiones del ámbito de aplicación

Portugal	España
▪ Estado Mayor General de las Fuerzas Armadas y ramas de las Fuerzas Armadas[3]. ▪ Entidades públicas con responsabilidades de investigación criminal y policías criminales y cuerpos de seguridad pública. ▪ Entidades públicas con responsabilidades exclusivas en la producción de información, a saber, el Sistema de	▪ Entidades de la Administración Pública que desarrollen actividades en los ámbitos de la seguridad nacional, la defensa nacional o la seguridad pública, incluida la prevención, investigación, detección y persecución de infracciones penales, excepto en las actividades en las que actúen como prestadores de servicios de confianza a disposición de terceros.

[2] Esto incluye proveedores de servicios de mercado en línea, de servicios de motores de búsqueda en línea y de servicios de plataformas de redes sociales.

[3] En lo que respecta a las redes y sistemas de información directamente relacionados con su mando y control.

Portugal	España
Inteligencia de la República Portuguesa, el Servicio de Inteligencia de Defensa Estratégica y el Servicio de Inteligencia de Seguridad. ▪ Entidades públicas cuya actividad se centre en redes y sistemas de información directamente relacionados con la producción y difusión de información clasificada, concretamente con marcas nacionales, de la Organización del Tratado del Atlántico Norte (OTAN) y de la Unión Europea, o catalogados como secretos de Estado, en relación con estas redes y sistemas de información. ▪ Otras entidades públicas que desarrollan su actividad en los ámbitos de la seguridad nacional, la seguridad pública, la defensa y los servicios de inteligencia, en lo que respecta a las redes y sistemas de información directamente relacionados con las actividades de producción de información y prevención, investigación, detección y enjuiciamiento de infracciones penales. ▪ Entidades privadas que presten servicios exclusivamente a una o varias entidades previstas en los párrafos anteriores y en relación con estas actividades.	▪ Instituto de Crédito Oficial.

Ambas propuestas adoptan la misma metodología y criterios para la clasificación de las entidades cubiertas como entidades **esenciales**. La clasificación de entidades como entidades **importantes** también asume los mismos criterios de clasificación, y España también incluye municipios que tengan más de 20.000 habitantes y entidades de su sector público institucional. Por su parte, Portugal ha optado por incluir un artículo dedicado exclusivamente a las entidades públicas que no están calificadas como entidades esenciales o importantes, clasificándolas como entidades públicas relevantes y dividiéndolas en dos grupos, a los efectos de aplicar regímenes específicos en los términos de la propuesta y otras regulaciones emitidas por el Centro Nacional de Ciberseguridad.

Con respecto al régimen sancionador, también se pueden anticipar algunas diferencias:

Regimen sancionador

Infracción administrativa	Portugal	España
Muy grave	Cometida por una entidad esencial: ▪ De 2.000,00 € a 10.000.000,00 € o al 2 % de la facturación mundial anual, en el ejercicio anterior. ▪ De 350,00 € a 200.000,00 €, si lo practica una persona física. Cometida por una entidad importante: ▪ De 1.250,00 € a 7.000.000,00 € o un importe máximo no inferior al 1,4 % de la facturación anual en todo el mundo. ▪ De 350,00 € a 200.000,00 €, si la comete una persona física. Cometida por una entidad pública relevante (dependiendo de si forma parte del grupo A o B): De 8.000,00 € a 4.000.000,00 €.	Total: de 500.001,00 € a 2.000.000,00 €. Cometida por una entidad esencial: la multa puede ascender a 10.000.000,00 € o al 2 % de la facturación anual a nivel mundial, en el ejercicio anterior. Cometida por una entidad importante: la multa puede ascender a 7.000.000,00 € o a un importe máximo no inferior al 1,4 % de la facturación anual en todo el mundo.
Grave	Cometida por una entidad esencial: ▪ De 1.250,00 € a 5.000.000,00 € o el 1 % de la facturación mundial anual en el ejercicio anterior; ▪ De 250,00 € a 125.000,00 €, si la comete una persona física. Cometida por una entidad importante: ▪ De 875,00 € a 3.500.000,00 € o un importe máximo no inferior al 0,7 % de la facturación anual en todo el mundo; ▪ De 250,00 € a 125.000,00 €, si lo practica una persona física. Cometida por una entidad pública relevante (dependiendo de si forma parte del grupo A o B): De 5.000,00 € a 225.000,00 €.	Total: de 100.001,00 € a 500.000,00 €.
Leve	De 875,00 € a 45.000,00 €, si la comete una persona jurídica. De 250,00 € a 3.750,00 €, si la comete una persona física.	Total: de 10.000,00 € a 100.000,00 €.

En general, las propuestas son bastante similares en lo que respecta a las obligaciones previstas para las entidades incluidas en su ámbito de aplicación, y ambas propuestas reflejan un claro compromiso con la mejora de la ciberresiliencia, con aspectos destacados y matices que ponen de relieve las prioridades y los modelos institucionales de cada Estado miembro.

3. Resoluciones de las autoridades de protección de datos

Sancionado un Ayuntamiento por el envío del justificante de pago de una multa a un domicilio desactualizado

La AEPD resuelve el procedimiento sancionador contra un Ayuntamiento por el envío del justificante de pago de una multa de tráfico al domicilio desactualizado de la reclamante, lugar en el que reside su expareja.

El documento contenía datos personales de la denunciante, incluyendo matrícula del vehículo, fecha y lugar de la infracción. La reclamante había actualizado su dirección en la Dirección General de Tráfico (DGT) y la había comunicado al agente sancionador del ayuntamiento, pero el justificante fue remitido a una dirección antigua que constaba en la base de datos de multas desde 2013. El Ayuntamiento alegó que el justificante no formaba parte del procedimiento sancionador y que el sistema seleccionó automáticamente el domicilio al no haberse actualizado la información antes del pago.

La AEPD considera que se vulneraron los principios de integridad y confidencialidad (art. 5.1.f RGPD) y de exactitud (art. 5.1.d RGPD), al no adoptarse medidas técnicas y organizativas adecuadas para garantizar la seguridad y actualización de los datos. La resolución destaca que el boletín de denuncia entregado en mano, donde la afectada indicó expresamente su dirección actual, no fue tenido en cuenta por el sistema informático al generarse el justificante de pago. Este fue enviado automáticamente a una dirección antigua registrada en la base de datos de multas, sin que se realizara una consulta actualizada a la DGT.

Se declara, en consecuencia, la existencia de infracción muy grave conforme al art. 83.5.a RGPD y art. 72.1.a LOPDGDD, y se ordena la comunicación de la resolución al Defensor del Pueblo.

Se desestima el recurso de una compañía de telecomunicaciones contra una sanción por el duplicado fraudulento de tarjetas SIM

La AEPD ha desestimado el recurso de reposición interpuesto por una compañía de telecomunicaciones contra la resolución sancionadora de 8 de noviembre de 2024 que impuso una multa de 200.000 euros por infracción del artículo 6.1 del RGPD.

La sanción se originó tras la emisión fraudulenta de un duplicado de tarjeta SIM a un tercero, sin base jurídica válida ni consentimiento del titular. La entidad alegó haber seguido sus protocolos internos y actuado con diligencia, pero la AEPD concluyó que tales medidas fueron insuficientes para garantizar la licitud del

tratamiento. La Agencia subrayó que la responsabilidad del tratamiento recae en el operador, quien debe verificar adecuadamente la identidad del solicitante y asegurar que el tratamiento se ajuste al RGPD. Se rechazaron las circunstancias atenuantes invocadas por la entidad sancionada, como la cooperación con la AEPD, la ausencia de beneficios y la no afectación de datos sensibles, por no cumplir los requisitos exigidos. Además, se valoraron como agravantes la reincidencia en infracciones similares y la vinculación directa de la actividad empresarial con el tratamiento de datos personales.

La resolución enfatiza que la emisión de una SIM a un tercero sin autorización constituye un tratamiento ilícito, con potencial para facilitar fraudes graves como el acceso a cuentas bancarias o redes sociales. La AEPD reafirma la necesidad de sanciones disuasorias y efectivas, y recuerda que la responsabilidad proactiva exige no solo disponer de medidas, sino garantizar su eficacia en todo momento.

Una cadena de centros comerciales ha sido sancionada por varias brechas de datos personales y medidas de seguridad

La AEPD ha sancionado a una cadena de centros comerciales con tres multas que ascienden a un total de 3.200.000 euros por vulneraciones del Reglamento General de Protección de Datos (RGPD).

La resolución deriva de cinco brechas de seguridad notificadas entre enero y septiembre de 2023, que afectaron a un total de 118.895 personas. Los ataques, ejecutados mediante técnicas de *credential stuffing*, permitieron accesos no autorizados a datos personales como nombre, dirección, correo electrónico, fecha de nacimiento y credenciales de acceso. La AEPD concluyó que la entidad infringió el artículo 5.1.f) del RGPD (principio de integridad y confidencialidad), el artículo 32 (seguridad del tratamiento) y el artículo 34 (comunicación de brechas a los interesados).

La empresa alegó haber adoptado medidas técnicas y organizativas, como auditorías y doble factor de autenticación, pero la AEPD consideró que estas fueron tardías, insuficientes o no implementadas adecuadamente. Además, se constató que las comunicaciones enviadas a los afectados no cumplían con los requisitos del artículo 34 del RGPD, al omitir información esencial sobre la naturaleza de la brecha y las medidas adoptadas.

La AEPD valoró como agravantes la escala de los datos comprometidos, la negligencia en la gestión de la seguridad y la vinculación directa de la actividad empresarial con el tratamiento masivo de datos personales.

Multada una compañía de electricidad y gas por la contratación fraudulenta de servicios

La AEPD ha sancionado a una compañía de electricidad y gas con una multa de 100.000 euros por vulnerar el artículo 6.1 del Reglamento General de Protección de Datos (RGPD), al realizar un tratamiento ilícito de datos personales sin base legal.

La reclamación fue interpuesta por un particular que denunció haber sido dado de alta en contratos de suministro de gas, electricidad y servicios anexos sin su consentimiento. La entidad sancionada alegó que la contratación fue gestionada por una empresa colaboradora, actuando como encargada del tratamiento, y que esta actuó de forma fraudulenta y al margen de sus instrucciones.

No obstante, la AEPD concluyó que la compañía no ejerció un control adecuado sobre su encargado, incumpliendo su deber de supervisión y permitiendo un tratamiento de datos sin legitimación. A pesar de que se anularon los contratos y facturas tras la reclamación, la Agencia consideró que la empresa no acreditó haber actuado con la diligencia exigible. La resolución subraya que el responsable del tratamiento puede ser sancionado por actuaciones de sus

encargados cuando no se garantice el cumplimiento del RGPD.

La infracción fue calificada como muy grave conforme al artículo 72.1.b) de la LOPDGDD. La AEPD valoró como agravantes la naturaleza del tratamiento, el volumen de datos afectados y la vinculación de la actividad empresarial con el tratamiento masivo de datos personales.

Sanción de 200.000 euros a una comercializadora energética por la inscripción de un cliente en un fichero de morosidad antes de que la notificación de requerimiento fuese devuelta

La AEPD ha impuesto una sanción de 200.000 euros a una comercializadora energética por inscribir los datos de un cliente en un fichero sin cumplir los requisitos del artículo 20.1 de la LOPD-gdd, lo que supone un tratamiento de datos sin base legitimadora conforme al artículo 6.1 del RGPD.

El reclamante alegó no haber recibido requerimiento de pago ni información sobre la posible inclusión en sistemas de morosidad. Aunque la reclamada aportó un requerimiento de pago, este fue devuelto por Correos en fecha posterior a la inscripción en el fichero de morosos, evidenciando que esta se llevó a cabo sin confirmar la recepción o devolución del requerimiento. Por tanto, la AEPD concluye que no se cumplió con la obligación de informar previamente al afectado, como exige el artículo 20.1.c), que requiere que dicha advertencia se realice en el contrato o en el momento del requerimiento de pago.

La sanción se agrava por la naturaleza de la infracción con afectación a la solvencia del reclamante, la vinculación de la actividad de la reclamada con el tratamiento de datos personales y la negligencia al incluir los datos sin que la deuda cumpliera los requisitos legales.

Una empresa de telecomunicaciones en Alemania es sancionada por fallos en supervisión y seguridad

La Autoridad Federal de Protección de Datos alemana ha impuesto dos multas administrativas a una empresa de telecomunicaciones por un total de 45 millones de euros, además de una amonestación, debido a deficiencias graves en la supervisión de encargados del tratamiento y en la seguridad de su portal de servicios en línea.

La reclamada, que opera a través de tiendas físicas gestionadas por agencias asociadas que actúan como encargados del tratamiento, disponía de acuerdos de encargo del tratamiento, si bien estos no estaban debidamente supervisados y auditados. Esto derivó en vulnerabilidades en los sistemas informáticos que facilitaron el uso indebido de datos personales en casos de fraude. Por ello, se impuso una multa de 15 millones de euros y una amonestación por la insuficiente supervisión y las debilidades técnicas.

Además, se sancionó a la entidad con 30 millones de euros adicionales por fallos en los mecanismos de autenticación de su portal *online*, que, combinados con la atención telefónica, permitían el uso indebido de eSIMs.

La AEPD concluye que no procede el derecho de portabilidad de datos en el ámbito educativo público, pero estima una reclamación por respuesta extemporánea

La parte reclamante presentó reclamación frente a la Consejería de Educación de la Junta de Castilla y León por entender desatendido su derecho a la portabilidad de los datos personales de sus hijas, alumnas de diferentes centros educativos públicos, al no haber recibido respuesta alguna por parte de estos centros en el plazo de un mes marcado por la norma. En particular, los datos se

referían a las evaluaciones psicopedagógicas de las hijas durante los años 2018 a 2023.

En este sentido, la parte reclamante alega que los centros educativos de la Consejería cuentan con plataformas electrónicas que permiten la remisión directa de los datos de un responsable a otro, por lo que la Consejería puede poner a disposición la documentación citada mediante el sistema de notificación electrónica. Por su parte, la reclamada manifiesta que la documentación solicitada se encuentra a disposición de la reclamante en los respectivos centros educativos, al no poder remitir datos de salud a correos particulares, como es el caso del centro privado de psicología al que se solicita la portabilidad.

En su resolución, la AEPD entiende que, al estar ante una relación (colegio público-padres) de índole administrativa y no contractual, regulada por tanto por la normativa pública de educación, el derecho a la portabilidad de los datos no alcanza al supuesto, ello con base en el considerando 68 y el artículo 20 del RGPD.

i. Considerando 68 del RGPD, "dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable".

ii. Artículo 20 del RGPD: "tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento".

La AEPD concluye que no procede atender el derecho de portabilidad en este caso, pero estima la reclamación por motivos formales al haberse emitido la respuesta extemporáneamente, si bien reconoce que no procede la realización de actuación adicional alguna por la reclamada.

Multado con 300 euros un empleado como responsable de una infracción consistente en el tratamiento de datos personales sin base legal alguna

En un primer momento, una persona física interpuso una reclamación frente a una entidad dedicada a la venta al por menor de frutas y hortalizas por haber sido contactada mediante unos mensajes de WhatsApp de índole personal por parte de un trabajador de la empresa. La reclamante entendió que el empleado obtuvo sus datos de entre los que ella aportó para la gestión de la tarjeta "Salamanca Tarjeta Activa", utilizada para obtener descuentos en comercios locales.

Durante el trámite de alegaciones, la entidad reclamada manifestó haber obtenido los datos directamente de la reclamante, alegando que es una cliente recurrente que realiza pedidos expresos para los cuales se le ha de contactar, así como que la reclamante participa activamente en un sorteo de Navidad para el cual es necesario dejar sus datos. No obstante, pese a que en un primer momento se archivó la reclamación, la reclamante recurrió en reposición, negando rotundamente lo alegado por la parte contraria, destacando la naturaleza personal de los mensajes enviados y haciendo referencia a la falta de acreditación de lo expuesto por la parte reclamada.

La AEPD resolvió estimar el recurso y ordenar la continuación del procedimiento, acordando llevar a cabo actuaciones de investigación para determinar la autoría y el origen del tratamiento. En este sentido, la AEPD determinó que la persona que se comunicó con la reclamante era efectivamente un empleado de la empresa, que lo hizo desde un teléfono móvil personal y que, además, el origen de los datos se encontraba, tal como alegaba la reclamante, en la cesión de datos desde la plataforma que gestionaba la tarjeta "Salamanca Tarjeta Activa" a los negocios

colaboradores, entre los que se encontraba la entidad reclamada.

Por tanto, la AEPD decide incoar un procedimiento sancionador y, a la luz de los hechos, concluye que el empleado utilizó los datos personales que la reclamante había proporcionado a la entidad reclamada por motivos profesionales, y no al empleado de esta por motivos personales. En consecuencia, se deduce que el empleado actuó a título personal y no por cuenta o siguiendo instrucciones del empleador, de forma que las operaciones de tratamiento realizadas no pueden ampararse en la base de licitud contractual con que cuenta la entidad. Finalmente, la AEPD resuelve imponiendo al empleado una sanción de 300 euros por una infracción del artículo 6.1 del RGPD, tipificada en el artículo 83.5.a) del RGPD.

La AEPD archiva una reclamación por la instalación de una mirilla digital al no apreciarse infracción en materia de protección de datos

El 19 de junio de 2025, la AEPD resuelve un procedimiento que trae causa en una reclamación interpuesta por un vecino de una comunidad de propietarios frente a otro, alegando que este último había instalado una mirilla digital en su puerta sin contar con autorización previa por la junta de propietarios. Igualmente, manifiesta que dicho instrumento es susceptible de grabar imágenes de zonas comunes, así como que no se encuentra debidamente señalizado.

La AEPD decide acordar el archivo de las actuaciones siguiendo unos criterios generales en relación con las mirillas digitales: (i) están permitidas siempre que cumplan una función similar a una mirilla tradicional; (ii) no es necesario para su instalación solicitar permiso a la junta de propietarios; (iii) la zona a que se dirigen (rellanos) no forma parte de la esfera íntima de las personas, siendo zonas de mero tránsito; y (iv) por lo general, las mirillas digitales no almacenan dato alguno, de manera que no es preceptivo informar de su presencia mediante señalización. Todo ello se suma al hecho de que la prueba de cargo aportada ha resultado insuficiente para desvirtuar la presunción de inocencia reconocida al reclamado.

Multa de 1,1 millones de euros a una empresa farmacéutica finlandesa por deficiencias en la protección de los datos de su tienda 'online'

La empresa farmacéutica sancionada utilizó *cookies* y otras tecnologías de seguimiento en su farmacia *online* que transmitían directamente a empresas como Meta o Google paquetes de datos de los usuarios, entre los que se encontraban interacciones de estos con diferentes medicamentos con receta y de venta libre, así como direcciones IP y otros datos que podrían permitir la identificación de los usuarios.

De esta forma, si un usuario estaba conectado a su cuenta de Google o Facebook cuando utilizaba la farmacia en línea, Google y Meta podrían haberlo identificado directamente. Todo ello cobra una mayor relevancia por la especial sensibilidad de los datos, al estar relacionados con aspectos de salud de las personas.

En este sentido, la autoridad finlandesa considera que la empresa ha infringido los artículos 5, 25 y 32 del RGPD por falta de medidas técnicas y organizativas apropiadas, e impone a la farmacéutica una sanción administrativa consistente en una multa por un importe de 1,1 millones de euros.

Un particular es multado por instalar cámaras orientadas hacia la vivienda de un vecino

La AEPD ha sancionado a un particular por la instalación de cámaras de videovigilancia orientadas hacia la entrada principal y la piscina de la vivienda colindante. La reclamación se remonta a más de cuatro años atrás, cuando la parte afectada denunció ante la AEPD que la presencia de las cámaras suponía una intromisión en su intimidad. En 2019, el reclamante intentó sin éxito una mediación a través del ayuntamiento

correspondiente. Posteriormente, la AEPD intentó solicitar a la persona reclamada que informara de las medidas adoptadas, pero el traslado no llegó a realizarse por incidencias en la entrega. Finalmente, en septiembre de 2024, se abrió procedimiento sancionador.

La persona reclamada alegó que las cámaras instaladas en el exterior de su domicilio carecían de grabación y de servicio de videovigilancia, y que su única finalidad era disuasoria frente a robos o actos vandálicos. Una inspección de los Mossos d'Esquadra confirmó que las cámaras no estaban operativas.

Sin embargo, en su resolución la AEPD advierte que la mera posibilidad de captar imágenes de espacios ajenos, aunque no se graben, constituye un tratamiento de datos personales, y considera que esta situación afecta a la intimidad de los afectados, genera una percepción de vigilancia y supone una medida desproporcionada al no limitarse a la protección de la propiedad propia. En consecuencia, la AEPD concluye que se ha vulnerado el artículo 5.1.c del RGPD, por la que impone una sanción de 500 euros.

Multa de 100.000 euros a una empresa logística por exigir antecedentes penales y datos personales excesivos en procesos de selección

La AEPD ha sancionado con 100.000 euros a una empresa dedicada a la logística, almacenamiento y transporte de mercancías por exigir información indebida a candidatos en procesos de selección. Un reclamante denunció que, para poder realizar una entrevista de trabajo, se le pidió presentar un certificado de antecedentes penales y cumplimentar un formulario en el que debía indicar su estado civil y número de hijos.

La compañía reclamada alegó que la solicitud del certificado se justificaba en el Reglamento de Ejecución (UE) 2015/1998, que exige comprobaciones de antecedentes penales para el personal con acceso a zonas de carga aérea, y que los datos de estado civil y descendencia se pedían para cumplimentar el modelo 145 de la Agencia Estatal de Administración Tributaria, relativo a la comunicación de datos del perceptor de rentas del trabajo. Sin embargo, en su resolución la AEPD considera que la normativa europea solo autoriza la verificación de antecedentes penales respecto de las personas finalmente seleccionadas para el puesto, no respecto de todos los aspirantes en fase de entrevista, por lo que la práctica de solicitar este certificado a todos los candidatos supone un tratamiento masivo e injustificado de datos relativos a condenas penales. Finalmente, respecto a los datos solicitados para el modelo 145, la Agencia aclara que únicamente deben recabarse una vez formalizada la relación laboral, no durante el proceso de selección.

Por todo ello la AEPD concluye que la empresa vulneró el artículo 5.1.c) del RGPD (relativo al principio de minimización de datos), así como el artículo 10 del mismo Reglamento y el artículo 10 de la LOPD-gdd, en relación con el tratamiento de datos penales. Por ello, impone dos sanciones: 75.000 euros por la solicitud indebida de antecedentes penales y 25.000 euros por la recogida anticipada de datos personales

Sancionada una entidad con 32.000 euros por divulgar datos médicos de un trabajador a un tercero

La AEPD ha sancionado a una entidad del ámbito de la prevención de riesgos laborales con una multa de 40.000 euros, reducida a 32.000 euros por pago voluntario, por vulnerar el principio de confidencialidad en el tratamiento de datos personales, conforme al artículo 5.1.f) del RGPD.

El procedimiento se inició tras la reclamación de un trabajador que, al acceder a su informe médico a través de la plataforma web del servicio de prevención, descubrió que el documento incluía pruebas médicas pertenecientes a otro empleado. El incidente se produjo por un error en el proceso de escaneo y subida de documentos, lo que permitió el acceso no autorizado a información especialmente sensible.

La AEPD consideró que la entidad no aplicó medidas organizativas adecuadas para evitar este tipo de situaciones, lo que supuso una pérdida de control sobre los datos personales por parte del afectado. Aunque la empresa alegó que se trató de un error humano y presentó medidas correctoras como formación del personal, revisión de protocolos y certificaciones de seguridad, la Agencia concluyó que estas acciones fueron adoptadas a posteriori y no eximen de responsabilidad.

La infracción fue calificada como muy grave, dado que afectó a datos de salud, considerados especialmente protegidos por la normativa. Aunque se valoró inicialmente una posible infracción del artículo 32 del RGPD (seguridad del tratamiento), esta fue archivada al no quedar acreditada la inexistencia de medidas técnicas generales.

Una entidad es multada con 180.000 euros por incumplir una resolución firme de la AEPD

La AEPD sancionó a una entidad con una multa de 225.000 euros, reducida a 180.000 euros por pago voluntario, por incumplir una resolución firme que le ordenaba atender el derecho de acceso ejercido por un interesado conforme al artículo 15 del RGPD.

El procedimiento se originó tras la reiterada negativa de la entidad a responder a los requerimientos de la AEPD, que le instaban a proporcionar al reclamante una certificación de acceso o una denegación motivada en un plazo de diez días hábiles. A pesar de múltiples requerimientos entre marzo y octubre de 2024, la empresa no acreditó haber cumplido con la resolución, lo que llevó a la AEPD a iniciar un procedimiento sancionador por vulneración del artículo 58.2 del RGPD, que obliga a cumplir las órdenes de la autoridad de control.

La entidad alegó confusión entre procedimientos similares y ausencia de intención de incumplir, pero la AEPD desestimó estas justificaciones, recordando que el cumplimiento de resoluciones firmes es exigible independientemente de errores internos. Además, calificó la infracción como muy grave según el artículo 72.1.m) de la LOPD-gdd, y destacó la importancia del principio de responsabilidad proactiva, que obliga al responsable del tratamiento a garantizar y demostrar el cumplimiento del RGPD durante todo el ciclo de vida del tratamiento.

La sanción fue graduada considerando factores como la duración del incumplimiento (más de un año), la reiteración de requerimientos y el hecho de que afectaba a un único interesado. Finalmente, la entidad optó por el pago voluntario, lo que permitió la terminación anticipada del procedimiento.

La AEPD respalda la conservación de datos personales por parte de un encargado del tratamiento una vez finalizado el encargo

En este caso, un encargado del tratamiento se oponía a eliminar los datos personales objeto del encargo una vez finalizada la relación contractual con el responsable del tratamiento. En su lugar, el encargado procedió a conservar los datos bloqueados, al alegar que esto era necesario para garantizar el adecuado ejercicio del derecho de defensa de sus intereses legítimos, al verse implicado en una controversia frente, precisamente, al responsable.

La AEPD, en su resolución, considera que la previsión del artículo 33.4 de la LOPD-gdd ampara esta actuación al indicar: “El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento”, por lo que, conjugando esta disposición con el derecho a la tutela judicial efectiva, la AEPD resuelve archivar el caso.

Si bien la AEPD no entra a desarrollar en detalle conceptos interesantes que surgen en la resolución -como es el del bloqueo- ni a concretar en detalle las implicaciones regulatorias de la conservación de estos datos por el encargado fuera del marco del contrato

de encargo (por ejemplo, haciendo referencia a su rol en ese momento, el deber de información para con los interesados, las bases legales en juego en este contexto, etc.), es una resolución a tener en cuenta, ya que saca a relucir un asunto muy común en la práctica, pero no muy habitualmente discutido en el sector, como es la habilitación prevista por el citado artículo 33.4 de la LOPD-gdd.

La AEPD estima que, para cumplir con el artículo 28 del RGPD, no es suficiente con indicar en el DPA que los datos se borrarán o devolverán al finalizar el tratamiento

En una sanción derivada de una brecha de seguridad sufrida por el encargado que prestaba servicios al responsable, la AEPD considera insuficiente la cláusula genérica que se suele incluir en los acuerdos de encargo de tratamiento por la que el encargado se obliga a suprimir o devolver los datos una vez finalice el servicio.

En este sentido, la AEPD estima que el responsable debe, si no lo indica de forma expresa en el contrato, impartir instrucciones claras y operativas para que el encargado respete los mismos plazos de conservación que rigen para el responsable, de manera que el encargado no retenga todos los datos hasta el fin del contrato cuando no sean necesarios.

La resolución impone al responsable una sanción de 250.000 euros por incumplimiento del art. 5.1 f) del RGPD y otra de 50.000 euros por incumplimiento del art. 28 RGPD.

La autoridad de control francesa sanciona a Google y Shein por instalación de 'cookies' y tecnologías similares sin consentimiento

La CNIL francesa ha impuesto dos sanciones históricas: 325 millones de euros a Google y 150 millones de euros a Shein, en el marco de su plan de acción sobre *cookies* y publicidad digital.

En el caso de Google, la autoridad detectó que la empresa insertaba anuncios con formato de correo electrónico en las pestañas "Promociones" y "Social" de Gmail sin obtener el consentimiento previo de los usuarios, lo que constituye prospección electrónica prohibida por la normativa francesa. Además, el proceso de creación de cuentas en Google no garantizaba un consentimiento válido para la instalación de *cookies* publicitarias, ya que la información era insuficiente y se dificultaba la opción de rechazo.

Por su parte, Shein fue sancionada por instalar *cookies* publicitarias en los dispositivos de los usuarios antes de que estos pudieran expresar su consentimiento, y por utilizar *banners* informativos incompletos que no explicaban adecuadamente las finalidades publicitarias ni identificaban a los terceros implicados. La CNIL también constató que, incluso tras rechazar las *cookies* o retirar el consentimiento, se seguían instalando y leyendo rastreadores.

Ambas resoluciones subrayan la importancia de obtener un consentimiento previo, libre e informado antes de cualquier tratamiento de datos con fines publicitarios, así como de ofrecer mecanismos de rechazo tan accesibles como los de aceptación. La CNIL advierte que seguirá vigilando activamente el cumplimiento, especialmente frente a prácticas engañosas o desproporcionadas en el diseño de *banners* y flujos para obtener el consentimiento de los interesados.

La AEPD no avala el uso de la fotografía de empleados para el control horario

La AEPD analiza la legalidad del sistema de control de jornada implantado por RENFE INGENIERÍA Y MANTENIMIENTO SME, S.A., que combina el uso de tarjeta identificativa y la toma de fotografía en el momento del fichaje, diferenciando entre oficinas centrales (solo tarjeta) y bases de mantenimiento (tarjeta y fotografía).

Conforme al artículo 4 del RGPD, la fotografía constituye un dato personal, pero no es un

dato biométrico, ya que no se emplean medios técnicos específicos para la identificación automática, sino que la verificación es manual por parte de Recursos Humanos. Se examina el cumplimiento de los principios del artículo 5 RGPD, especialmente los de licitud, minimización, limitación de finalidad y seguridad, y la base jurídica para el registro de jornada, que es el cumplimiento de una obligación legal, la prevención del fraude y la gestión de la relación contractual a través del control de la actividad laboral (artículos 20.3 y 34.9 del Estatuto de los Trabajadores).

Se acredita que la información a los trabajadores es adecuada y que el tratamiento es necesario y proporcional, descartando métodos alternativos más intrusivos. Por tanto, no se aprecia infracción, pues el sistema no vulnera los principios del RGPD ni implica tratamiento de datos biométricos, procediéndose al archivo de actuaciones.

Sancionado un club de fútbol por una brecha de seguridad causada por un ataque de 'ransomware'

La AEPD sanciona a un club de fútbol por una brecha de seguridad causada por un ataque de *ransomware* que afectó a datos personales de aproximadamente 60.000 personas, incluyendo datos especialmente protegidos.

La AEPD fundamenta su competencia en el artículo 58.2 del RGPD y la LOPD-gdd, y señala que la entidad, como responsable del tratamiento, debe garantizar la integridad y confidencialidad de los datos (art. 5.1.f RGPD), así como aplicar medidas técnicas y organizativas adecuadas al riesgo (art. 32 RGPD).

La resolución constata la ausencia de medidas suficientes, como la falta de segmentación de red y de cifrado de datos, lo que permitió que el ataque comprometiera la totalidad de los servidores virtualizados y las copias de seguridad. Se destaca la gravedad de la infracción por el volumen y la sensibilidad de los datos afectados, así como la duración de la brecha.

La conducta se califica como infracción muy grave (art. 83.5 RGPD y art. 72 LOPD-gdd) y grave (art. 83.4 RGPD y art. 73 LOPD-gdd), imponiéndose una sanción total de 110.000 euros, reducida a 66.000 euros por reconocimiento de responsabilidad y pago voluntario. Se ordena, además, la adopción de medidas correctivas para adecuar la seguridad al RGPD.

La AEPD sanciona a una empresa tecnológica por la cesión de datos personales a terceros sin contar con una base legitimadora suficiente

La entidad reclamante, una asociación que promueve la democracia y los derechos digitales, interpuso una reclamación ante la AEPD contra una empresa tecnológica, alegando que los datos personales de trabajadores autónomos facilitados a la AEAT y al Registro Mercantil para su alta en el censo de actividades económicas fueron posteriormente tratados y cedidos a terceros -incluyendo la Cámara de Comercio, Camerdata y consultoras privadas- para fines comerciales y de *marketing*, sin base legal suficiente y sin que los interesados hubieran sido debidamente informados. La reclamación subrayaba que dichos datos, entre los que se incluían identificadores como el NIF, quedaron accesibles en internet y se utilizaron para finalidades ajenas a las inicialmente informadas.

Durante la instrucción, la AEPD recabó información de las entidades implicadas. La entidad denunciada defendió la licitud del tratamiento invocando el interés legítimo, la procedencia de fuentes públicas y la adopción de medidas informativas indirectas. Sin embargo, la AEPD concluyó que el tratamiento excedía el marco legal previsto en la Ley 4/2014 de Cámaras, al destinarse a la comercialización masiva de bases de datos para campañas de *marketing*, y que la presunción de licitud del artículo 19 LOPD-gdd no amparaba el uso de datos identificativos como el NIF. Asimismo, apreció el incumplimiento del deber de información del artículo 14 RGPD, al no garantizarse que los interesados fueran efectivamente informados.

En consecuencia, la AEPD estimó la reclamación, declaró infringidos los artículos 6.1 y 14 RGPD, impuso sanciones de 24.000 y 18.000 euros respectivamente, y ordenó el cese del tratamiento y la supresión de los datos tratados sin base legítima.

Multada una empresa de viajes por vulneración del principio de minimización de datos

La resolución trae causa de una reclamación interpuesta ante la AEPD contra una compañía de viajes por considerar que la entidad había solicitado indebidamente una copia completa del documento de identidad de los huéspedes durante el proceso de *check-in online* para una reserva de alojamiento, lo que suponía, a juicio del reclamante, una petición excesiva de datos personales.

En concreto, el reclamante alegó que, si bien facilitó los datos identificativos requeridos, la parte reclamada insistió en la necesidad de remitir copia íntegra del documento de identidad, alegando que era imprescindible para cumplir con las obligaciones legales de registro y comunicación a las fuerzas de seguridad. Por su parte, la parte reclamada alegó que solicitaba la imagen completa del documento de identidad de los huéspedes como parte del proceso de verificación de identidad, en cumplimiento del Real Decreto 933/2021, justificando que la comprobación presencial no era viable en su modelo de negocio digital.

No obstante, la AEPD, tras analizar la normativa aplicable y el principio de minimización de datos del RGPD, consideró que la solicitud de una copia completa del documento de identidad excedía los datos estrictamente necesarios para la finalidad perseguida, ya que la normativa únicamente exige la recogida de determinados datos identificativos y no la copia íntegra del documento. En consecuencia, la AEPD estimó la reclamación, considerando que la parte reclamada había vulnerado el principio de minimización de datos previsto en el artículo 5.1.c) del RGPD, imponiendo una sanción administrativa de 70.000 euros, que fue reconocida y abonada voluntariamente por la parte reclamada, por lo que se vio reducida a 42.000 euros. Asimismo, le requirió la adopción de medidas correctivas para adecuar sus procedimientos, eliminando la exigencia de aportar copia del documento de identidad y suprimiendo las imágenes ya recabadas.

La Autoridad polaca de protección de datos impone sendas multas a responsable y encargado por negligencia en el análisis de riesgos y en la adopción de medidas de seguridad

La Autoridad de Protección de Datos de Polonia ha sancionado a una cadena de restaurantes con una multa de 4.022.773 euros y a uno de sus encargados del tratamiento con 43.680 euros, tras constatar graves deficiencias en el análisis de riesgos y en la adopción de medidas de seguridad en el tratamiento de datos personales.

El caso se originó a causa de la notificación de una brecha de seguridad que expuso datos sensibles de empleados y franquiciados en un archivo que era accesible al público. La investigación reveló que ni el responsable ni el encargado del tratamiento realizaron un análisis de riesgos adecuado ni implementaron medidas técnicas y organizativas proporcionales a la naturaleza y escala del tratamiento, incumpliendo así los artículos 24, 25, 28, 32 y 38 del RGPD. Además, el encargado subcontrató servicios sin el preceptivo acuerdo de subencargado del tratamiento, y adicionalmente el delegado de protección de datos no estuvo debidamente involucrado en la gestión de la seguridad, lo que limitó la capacidad preventiva de la organización.

La resolución subraya la importancia de la supervisión efectiva, la actualización continua de las medidas de seguridad y la implicación activa del delegado de protección de datos en todos los procesos relacionados con la protección de datos.

4. Sentencias

La Audiencia Nacional avala una sanción de la AEPD por tratamiento sin base legitimadora al publicar listados con nombres y apellidos de opositores

La Audiencia Nacional confirma la sanción de 12.000 euros impuesta a una sociedad por la AEPD en agosto de 2022 por publicar en su página web listados de resultados de un proceso selectivo celebrado en el marco de concurso-oposición convocado por el Servicio Gallego de Salud (SERGAS), con nombres y apellidos y sin el consentimiento de los afectados.

El conflicto surge a raíz de que en la publicación realizada por la entidad se modificaron las listas de puntuaciones provisionales del proceso selectivo para el Grupo Auxiliar de la Función Administrativa del SERGAS, inicialmente publicadas oficialmente por esta entidad en 2019. Mientras que las listas originales se disponían en orden alfabético y mezclaban diferentes turnos, la entidad sancionada reorganizó los datos por puntuaciones y las clasificó en tres categorías: "Acceso Libre", "Discapacidad General" y "Promoción Interna". Estos listados incluían nombres y apellidos de los aspirantes, lo que, según la AEPD, supuso un tratamiento indebido de datos personales, dado que no se ajustaba a los fines legítimos de la publicación original.

La sentencia rechaza los argumentos de la empresa sobre la anonimización, el interés legítimo y la proporcionalidad de la sanción, concluyendo que su actuación no estaba amparada por la normativa, al tratarse de un tratamiento adicional de datos sin base legal adecuada. Según la sentencia, el hecho de alterar el formato original de los datos personales y clasificarlos por puntuación, en lugar de seguir la disposición alfabética establecida oficialmente, alteró la finalidad original del tratamiento, vulnerando los principios del RGPD. En particular, la Sala destacó que no existía consentimiento expreso de los afectados ni otro fundamento jurídico válido que legitimara esta reconfiguración de los datos personales.

Por consiguiente, la sentencia desestima el recurso contencioso-administrativo interpuesto por la entidad sancionada y confirma en su totalidad la resolución de la AEPD, que imponía la sanción ya citada de 12.000 euros.

El TSJ de Galicia analiza el uso de algoritmos en procesos de selección y confirma la discriminación sindical en una autoridad portuaria

Esta sentencia del Tribunal Superior de Justicia de Galicia resuelve un recurso de suplicación presentado por una autoridad portuaria contra un fallo dictado por un Juzgado de lo Social en relación con la demanda de tutela de derechos fundamentales iniciada por un particular. En

concreto, se discute si la entidad vulneró el derecho fundamental de libertad sindical en procesos relacionados con la movilidad funcional y el acceso a determinados puestos de trabajo en la organización, en conexión con el uso de algoritmos predictivos.

En 2017 la autoridad portuaria aplicó criterios de movilidad funcional para cubrir temporalmente diferentes posiciones laborales recurriendo a un sistema de perfiles y baremos técnicos para designar a los candidatos, tomando en cuenta factores como la distancia técnica al perfil ideal del puesto.

La demandante alegó discriminación sindical en su contra durante estos procesos, ya que, aunque figuró en varias ocasiones como la candidata más idónea según los criterios objetivos de evaluación, la empresa optó por seleccionar a otros trabajadores. Según la demandante, las decisiones fueron desestimadas o alteradas considerando subjetivamente otros factores, como la influencia de posiciones sindicales, señalando que su rol como secretaria del Comité de Empresa y su afiliación sindical habrían jugado en su contra.

La empresa demandada no consiguió probar las verdaderas razones por las que se había apartado del criterio algorítmico, por lo que el tribunal declaró que efectivamente la empresa vulneró el derecho fundamental a la libertad sindical, decretando la nulidad del nombramiento de uno de los candidatos seleccionados y reconociendo el derecho de la demandante a percibir las diferencias salariales correspondientes al puesto que legítimamente le correspondía. Ante esta resolución, la autoridad portuaria presentó un recurso de suplicación, llevando el caso a una segunda instancia para su revisión, que finalizó reafirmando que hubo discriminación sindical en perjuicio de la demandante.

En resumen, la sentencia sienta un importante precedente sobre la garantía de los derechos fundamentales en el ámbito laboral, particularmente en lo relativo a la libertad sindical y la transparencia en los procesos internos de selección en organizaciones públicas.

La Corte Suprema de Chile ordena a una empresa de telecomunicaciones indemnizar a un cliente por vulneración de datos personales

La Corte Suprema de Chile condenó a una empresa de telecomunicaciones a pagar una indemnización de siete millones de pesos a un cliente cuya identidad fue utilizada por estafadores para contratar cinco líneas telefónicas sin su consentimiento. El fallo determinó que la empresa no cumplió con su deber de proteger los datos personales del afectado, lo que facilitó el fraude. La compañía fue responsabilizada por no verificar adecuadamente la identidad de quienes realizaron los contratos, vulnerando la Ley de Protección de Datos Personales.

La sentencia marca un precedente en la protección de datos personales en Chile, sancionando a la compañía por vulnerar la ley y facilitar un fraude.

Caso Latombe: El TGUE valida el esquema de transferencias internacionales UE – EE.UU.

El Tribunal General de la Unión Europea (TGUE) ha dictado sentencia en el conocido como “Caso Latombe”, que tenía por objeto un recurso de anulación interpuesto por el eurodiputado Philippe Latombe frente al esquema de transferencias internacionales a los EE.UU. actualmente en vigor.

Uno de los principales puntos de esta sentencia gira alrededor de la independencia del Data Protection Review Court (DRPC) de los EE.UU., que actuaría como tribunal de recurso en relación con materias de protección de datos en dicha jurisdicción. Según el criterio del Sr. Latombe, este

DPRC no opera de modo imparcial ni independiente, a resultas de su dependencia del poder ejecutivo. No obstante, el TGUE considera que el DPRC actúa bajo una serie de garantías y conforme a ciertas normas que ofrecen suficientes evidencias de independencia funcional de sus miembros. Así, junto con otras valoraciones adicionales, el TGUE desestima el recurso interpuesto.

Con esta resolución, el TGUE viene, en líneas generales, a ratificar el citado esquema, confirmando que este ofrece suficientes garantías como para asegurar un nivel de protección suficiente sobre los datos objeto de transferencia, evitando así -al menos de momento- una nueva anulación del esquema de regularización de estas transferencias, como ocurriera con los antiguos Privacy Shield o Safe Harbour.

En cualquier caso, y tal como indica el TGUE en su nota de prensa al respecto, la Comisión Europea deberá hacer un seguimiento del marco jurídico de las transferencias de datos a EE.UU., de modo que, si hubiera algún desarrollo o novedad que impacte en las garantías aplicables, la Comisión deberá decidir si modificar o dejar sin efecto este esquema.

La Audiencia Nacional entiende que las solicitudes de acceso a los datos personales deben remitirse a los canales habilitados al efecto y no a direcciones genéricas

La parte recurrente interpuso recurso contencioso-administrativo ante la Audiencia Nacional contra una resolución de la AEPD que inadmitió su reclamación por no haber recibido respuesta a su solicitud de acceso a los datos personales y académicos tratados por una universidad. El reclamante había solicitado, a través de un correo electrónico enviado a una dirección genérica, el acceso a su expediente académico y, al no obtener respuesta, acudió a la AEPD. La Agencia inadmitió la reclamación al considerar que el interesado no utilizó los canales específicos habilitados por la universidad para el ejercicio de derechos de protección de datos, como la dirección de correo electrónico o postal indicada en la política de privacidad de la entidad.

La Audiencia Nacional, aplicando el artículo 15 del RGPD y el artículo 13 de la LOPD-gdd, confirma la decisión de la AEPD. La Sala considera que la universidad no limitó ni obstruyó el derecho de acceso, ya que el reclamante no acreditó haber presentado su solicitud a través de los cauces expresamente habilitados y publicados por la entidad para el ejercicio de derechos. En este sentido, señala que “fue el denunciante quien presentó su solicitud fuera de los cauces establecidos para ello, inobservando lo previsto al respecto en la página web de la entidad reclamada”.

En consecuencia, desestima el recurso, confirma la resolución de inadmisión de la AEPD y condena en costas al actor, advirtiendo de que la sentencia es susceptible de recurso de casación.

El TJUE analiza la posibilidad de comunicar datos de trabajadores desde una empresa a su matriz para probar un ‘software’ y declara ilícito el uso de datos reales sin base legal

El caso trata sobre el uso indebido de datos personales de un empleado por una empresa alemana, parte de un grupo internacional con sede en EE.UU.

En 2017, el grupo implementó un *software* de recursos humanos en la nube para pruebas, estableciendo contractualmente que solo se podrían emplear datos limitados (nombre, apellidos, fecha de incorporación, lugar de trabajo y teléfono profesional) y prohibiendo expresamente el uso de datos reales para fines de administración de personal. Sin embargo, la empresa subió a la nube datos sensibles del empleado, como salario, domicilio, fecha de nacimiento, estado civil, número de la seguridad social, nacionalidad e identificación fiscal, que fueron tratados hasta 2019.

El empleado demandó ante la jurisdicción laboral, argumentando que el uso de datos reales no era necesario para la finalidad de prueba y que se había excedido el marco permitido, solicitando una indemnización por daños no materiales. Tanto el tribunal laboral de primera instancia como el tribunal regional desestimaron la demanda.

Posteriormente, el Tribunal Federal del Trabajo planteó una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea (TJUE) sobre la interpretación del artículo 88.1 del RGPD en relación con la normativa laboral alemana. El TJUE recordó que las normas nacionales sobre tratamiento de datos en el ámbito laboral deben respetar plenamente las condiciones y límites del RGPD, especialmente los artículos 5, 6 y 9.

Finalmente, el tribunal concluyó que la empresa trató datos personales sin base legal, infringiendo el artículo 6.1 RGPD, y reconoció al empleado una indemnización de 200 euros por pérdida de control sobre sus datos (artículo 82.1 RGPD). Además, subrayó que el uso de datos reales en pruebas solo sería legítimo si los datos ficticios no fueran suficientes para el objetivo perseguido, cosa que no ocurría en este caso.

Los tribunales admiten el uso de imágenes de videovigilancia como medio de prueba en procesos penales

El Tribunal de Apelación de Évora en la sentencia del 3 de junio de 2025, Proc. 412/21.6JAFAR.E1, se pronunció sobre la admisibilidad del uso de imágenes captadas por un sistema de videovigilancia como medio de prueba en un proceso penal. Lo que estaba en juego era el uso de grabaciones obtenidas por cámaras instaladas fuera de un club nocturno, que capturaban la comisión de un delito. El tribunal entendió que las imágenes no invadían el núcleo de la vida privada del acusado y habían sido recogidas en un lugar público con el objetivo de documentar hechos penalmente relevantes, por lo que eran admisibles como prueba. La decisión se basa en el principio de justa causa y en la ausencia de vulneración del principio de proporcionalidad, afirmando que la protección conferida por el RGPD, aunque aplicable, no impone en este contexto una exclusión automática de pruebas.

Una sentencia aclara que el consentimiento del interesado no reemplaza a la autorización judicial cuando se trata de aportar pruebas en el marco de un proceso judicial

El Tribunal de Apelación de Oporto en la sentencia de 30 de abril de 2025, Proc. 875/24.8PDVNG-A. P1, analizó la posibilidad de utilizar, en un proceso penal, los datos de localización GPS instalados en un vehículo de motor. El caso se refería a la solicitud realizada por el Ministerio Público al operador de telecomunicaciones responsable, con el objetivo de obtener la ubicación de un vehículo robado. Aunque el titular del contrato dio su consentimiento para la recopilación, el operador se negó a entregar los datos sin intervención judicial. El tribunal confirmó la necesidad de autorización del juez de instrucción para la validación de las pruebas y para unirse al proceso penal, considerando que el uso de datos de ubicación en los procesos penales puede interferir con los derechos fundamentales, lo que requiere un control judicial previo. La decisión aclara que el consentimiento del titular no reemplaza el requisito de protección judicial cuando está en juego la admisibilidad procesal de los datos.

Dictamen de la CNPD sobre la transmisión por internet de las reuniones de los órganos locales

La CNPD emitió el Dictamen nº 29/2025 sobre la transmisión en línea de las reuniones de los órganos de las autoridades locales, a petición de la Junta Parroquial de Avenidas Novas. La CNPD

confirma el entendimiento ya adoptado en 2023, considerando que la transmisión en directo (audio y vídeo) en línea de estas reuniones no tiene un marco jurídico en el régimen jurídico de las autoridades locales ni en el principio de transparencia previsto en el RGPD.

Señala que, si bien la publicidad de las reuniones está prevista por ley, no implica que se transmitan por medios digitales. La transmisión en vivo, al exponer sistemáticamente imágenes, voces y opiniones de los participantes, puede violar el principio de minimización y representar un cambio en el propósito de la recopilación de datos. Por este motivo, la CNPD considera que este tipo de difusión constituye un tratamiento adicional que requiere una nueva base jurídica y, por regla general, una evaluación de impacto, destacando la necesidad de un cumplimiento escrupuloso del artículo 13 del RGPD, para que los interesados estén plena y claramente informados de este tratamiento.

El dictamen admite que la grabación y la posterior disponibilidad de las reuniones solo pueden llevarse a cabo sobre la base del consentimiento de los participantes, de conformidad con el artículo 6, apartado 1, letra a), del RGPD, siempre que se cumplan plenamente los requisitos aplicables al consentimiento y previstos en el RGPD. En este sentido, la CNPD ya había señalado que dicho consentimiento debe recogerse no solo en relación con quienes, en el ejercicio de sus funciones o en el ejercicio del derecho a participar, realizan declaraciones durante las reuniones, sino también en relación con quienes ejercen el mismo derecho de participación por mera presencia o asistencia en las mismas. Por último, la CNPD subraya la necesidad de distinguir entre los titulares de cargos públicos, cuyos datos pueden estar sujetos a menos expectativas de privacidad, y los ciudadanos intervinientes, cuyos datos requieren una mayor protección.

En 2023, la CNPD ya había publicado las directrices sobre la transmisión por Internet de las reuniones de los órganos locales, en las que se basa fundamentalmente el dictamen emitido.

5. Actualidad

El Reglamento de Datos de la Unión Europea ('Data Act') es aplicable desde el 12 de septiembre de 2025

Desde el 12 de septiembre de 2025 es aplicable en toda la Unión el Reglamento (UE) 2023/2854, conocido como *Data Act*, una norma clave para impulsar un mercado de datos más abierto y competitivo en Europa. El reglamento había entrado en vigor en diciembre de 2023, pero su aplicación general comienza ahora, con disposiciones que afectan a fabricantes de dispositivos conectados, proveedores de servicios *cloud* y a todo tipo de entidades que gestionan datos generados por el Internet de las Cosas (IoT).

El *Data Act* establece derechos concretos para los usuarios de productos y servicios conectados, al garantizarles el acceso y la reutilización de los datos generados por sus dispositivos. Asimismo, impone obligaciones de intercambio equitativo de datos entre empresas (*B2B*), habilita un acceso restringido por parte de organismos públicos en casos de emergencia o interés público excepcional, y promueve la interoperabilidad y portabilidad en los servicios *cloud*, con una reducción progresiva de los costes de cambio de proveedor.

El *Data Act* establece un calendario de aplicación progresiva. Desde el 12 de septiembre de 2025 ya son exigibles las obligaciones generales del reglamento, como las relativas a la transparencia en el acceso y compartición de datos o las normas contractuales para evitar cláusulas abusivas en acuerdos *B2B*. Posteriormente, a partir de septiembre de 2026, se activan requisitos técnicos más específicos, como la obligación de que los productos y servicios conectados estén diseñados para permitir el acceso directo a los datos por parte de los usuarios. Finalmente, en 2027 determinadas disposiciones se extenderán también a contratos anteriores de larga duración.

En todo momento, el *Data Act* se aplica en coordinación con el Reglamento General de Protección de Datos, cuya primacía se enfatiza de forma expresa, garantizando un equilibrio entre la economía de los datos, la innovación tecnológica y la salvaguarda de la privacidad.

Puedes consultar aquí el artículo "El *Data Act* entra en acción: claves de un mosaico normativo que ninguna empresa puede ignorar", de Begoña González Otero, of counsel de Propiedad Industrial e Intelectual de Garrigues y experta en derecho digital.

La Comisión Europea publica una resolución en la que se considera que Apple y Meta infringen el Reglamento de Mercados Digitales y se les imponen sanciones de 500 y 200 millones de euros, respectivamente

La Comisión ha dictado una resolución por la que sanciona a Meta y Apple por el incumplimiento de la *Digital Markets Act* (DMA).

En el caso de Apple, la Comisión ha determinado que la empresa ha vulnerado la obligación de permitir que los desarrolladores de aplicaciones informen gratuitamente a los usuarios sobre ofertas alternativas fuera de la *App Store*, así como la posibilidad de redirigirlos hacia ellas. Se impone una multa por importe de 500 millones de euros, así como la obligación de suprimir todas las restricciones técnicas y comerciales a la redirección y abstenerse de perpetuar la conducta en el futuro.

Por otro lado, en lo que se refiere a Meta -es aquí donde la resolución más colinda con el ámbito de la protección de datos personales-, se impone una sanción por incumplimiento del artículo 5.2 a), b) y c) de la *Digital Markets Act* por el uso del sistema "*pay or okay*" en relación con el tratamiento de datos para publicidad personalizada. Cabe destacar que la empresa ha introducido un nuevo modelo que está siendo actualmente analizado por la Comisión de cara a determinar su adecuación a la legalidad. Finalmente, la Comisión ha resuelto sancionar a Meta imponiendo una multa por importe de 200 millones de euros.

El CEPD publica la Declaración de Helsinki y anuncia nuevas medidas para simplificar y reforzar la aplicación del RGPD

El Comité Europeo de Protección de Datos (CEPD) ha hecho pública la denominada **Declaración de Helsinki sobre mayor claridad, apoyo y compromiso**, en la que anuncia un conjunto de iniciativas dirigidas a facilitar la aplicación práctica del RGPD y a reforzar la coherencia en su cumplimiento en toda la Unión Europea.

Entre las principales medidas anunciadas, se incluyen:

- **Simplificación de procedimientos**: elaboración de plantillas de referencia para las organizaciones, incluyendo una plantilla común de notificación de violaciones de datos personales a las autoridades de protección de datos.

- **Refuerzo de la coherencia**: recopilación y puesta en común de posturas adoptadas por las autoridades nacionales, resoluciones administrativas y sentencias judiciales, con el objetivo de elaborar publicaciones que funcionen como "jurisprudencia" de referencia para las organizaciones.

- **Coordinación inter regulatoria**: desarrollo de directrices conjuntas con otros organismos reguladores europeos para favorecer una aplicación coherente entre distintos marcos normativos que afectan a las entidades.

Con esta declaración, el CEPD busca responder a las demandas de mayor claridad normativa y de apoyo práctico a las organizaciones, al tiempo que promueve un marco homogéneo de cumplimiento del RGPD en toda la Unión.

Chile: La Comisión de Implementación para la nueva Ley de Protección de Datos publica tres informes

La Comisión Asesora Ministerial para la Implementación de la Ley de Protección de Datos Personales presentó tres informes este año con diversas recomendaciones para la puesta en marcha de esta nueva regulación en el país. El primer informe aborda la Agencia de Protección de Datos Personales (APDP), recomendando anticipar su operatividad a junio de 2026, además de recomendar el fortalecimiento de su estructura

y presupuesto para garantizar una protección efectiva de los datos personales.

El segundo informe orienta sus recomendaciones al ingreso de Chile a cadenas de valor digitales, fomentando la innovación y asegurando la confianza de inversionistas y socios comerciales. Dentro de ellas se encuentra la aprobación de normas corporativas vinculantes presentadas por empresas y de cláusulas contractuales tipo, así como la exploración de flujos de transferencia internacionales de datos con socios comerciales APEC. Asimismo, considera la declaración de países que proporcionen niveles adecuados de protección de datos, debiéndose iniciar los trámites de reconocimiento de Chile como país adecuado y el proceso de adhesión al Convenio 108+ del Consejo de Europa.

El tercer informe dirige sus recomendaciones al sector público y propone que la Secretaría de Gobierno Digital emita un oficio circular con lineamientos y guías técnicas para asegurar una implementación coordinada de la Ley de Protección de Datos Personales en los órganos de la Administración del Estado. Entre las medidas prioritarias, se destacan la designación de delegados de protección de datos, la creación de comités internos de implementación, la adopción de políticas de tratamiento y de procedimientos para el ejercicio de los derechos ARCO, y la implementación de medidas de seguridad y planes de capacitación, entre otras.

El EDPB adopta las directrices 3/2025 sobre la interacción entre la DSA y el RGPD

El Comité Europeo de Protección de Datos (EDPB) adoptó el 12 de septiembre de 2025 sus Directrices 3/2025 para aclarar cómo se coordinan la *Digital Services Act* (DSA) y el RGPD.

El EDPB subraya que la DSA persigue objetivos distintos y complementarios, no deroga al RGPD ni crea por sí misma una base jurídica autónoma para tratar datos personales: cuando el cumplimiento de la DSA implique tratamiento de datos, los proveedores deben identificar una base del artículo 6 del RGPD y respetar los principios de minimización, limitación de la finalidad y proporcionalidad.

Las directrices bajan al detalle en áreas sensibles. En los sistemas de "*notice and action*" y de reclamaciones internas (arts. 16, 17, 20 y 23 DSA) solo deben tratarse los datos estrictamente necesarios y, cuando proceda, la identidad del notificante solo se comunica si es imprescindible, con salvaguardas adecuadas. Además, cualquier decisión automatizada debe respetar las restricciones del RGPD, incluidas las relativas a categorías especiales de datos. En diseños con patrones engañosos (*dark patterns*), el EDPB recuerda que el artículo 25 DSA debe leerse junto al RGPD: no puede manipularse el consentimiento ni otras elecciones sobre el tratamiento de los datos personales; y está prohibida la publicidad basada en categorías especiales de datos, incluso si, en abstracto, existiera base jurídica o una excepción del artículo 9.2 del RGPD.

Para plataformas y motores de búsqueda de muy gran tamaño (VLOPs/VLOSEs), el EDPB enfatiza la gestión de riesgos sistémicos de la DSA acompañada de protección de datos desde el diseño y por defecto y, cuando proceda, evaluaciones de impacto (DPIA) bajo el RGPD. Recomienda evitar mecanismos de *age assurance* que identifiquen de forma inequívoca a usuarios o almacenen permanentemente la edad; y pide coordinación estrecha entre los *digital services coordinators*, la Comisión y las autoridades de protección de datos, así como su participación en la elaboración de códigos de conducta de la DSA para asegurar coherencia con los del artículo 40 del RGPD.

Memoria anual 2024 de la AEPD: principales resultados y tendencias

La AEPD ha publicado su Memoria 2024 con un panorama mixto: bajan las reclamaciones resueltas, pero suben tanto el importe total de las sanciones como la presión sancionadora en sectores clave. En 2024 se impusieron 281

multas (−23 % respecto a 2023) por un importe agregado de 35,6 millones de euros (+19 %). Lideran el importe sancionado los sectores de energía/agua, entidades financieras, servicios de internet, telecomunicaciones y contratación fraudulenta. La sanción más elevada del año, de 5 millones de euros, se impuso por falta de transparencia en la información ofrecida a los usuarios, ausencia de una base jurídica válida para determinados tratamientos y deficiencias en el cumplimiento de los principios de licitud y lealtad en el uso de los datos personales.

En el ámbito de las brechas de datos personales, la Agencia recibió 2.933 notificaciones (+ 46% anual). El 84 % procedió del sector privado y el 16 % del sector público, con más de 100 millones de personas potencialmente afectadas. Los procedimientos vinculados a brechas acumularon más de 13 millones de euros en sanciones.

En materia de tramitación, la AEPD resolvió 18.132 reclamaciones en 2024 (−11 % interanual). La figura del delegado de protección de datos siguió consolidándose: 206 delegados se certificaron en 2024 (acumulado de 1.306), con 11.227 delegados comunicados que cubren a 119.803 responsables. De ellos, el 11,63 % ya cuenta con certificación oficial. Por último, la atención a la ciudadanía experimentó un fuerte crecimiento, con 98.162 consultas atendidas (+42,5 %), reflejando una mayor demanda de orientación en materia de protección de datos.

La Comisión Europea ha publicado un informe sobre la aplicación de la Estrategia de Salud Mundial de la UE

Tras la entrada en vigor del Reglamento (UE) 2025/327 por el que se crea el Espacio Europeo de Datos Sanitarios (EEDS), la Comisión Europea publicó el 10 de julio de 2025 un informe sobre la aplicación de la Estrategia de Salud Mundial de la UE [COM(2025) 392].

Este informe presenta las principales acciones tomadas y los avances realizados en temas prioritarios para la mejora de la salud global. En particular, destaca los avances logrados en la implementación de la Estrategia Mundial de Salud, centrada en tres grandes prioridades: la promoción de la salud, el fortalecimiento de los sistemas de salud, y la protección contra amenazas para la salud.

El informe está dirigido al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, y proporciona información sobre las medidas adoptadas, los resultados obtenidos y los retos en la aplicación de la estrategia sanitaria global de la UE.

En particular, el informe destaca el fortalecimiento de la gobernanza de los datos de salud. En este sentido, se menciona que uno de los objetivos de la Estrategia de Salud Global de la UE es aprovechar que la UE es pionera en la regulación de datos sanitarios y certificados digitales, utilizando el almacenamiento en la nube para el intercambio de datos, la protección de datos y la privacidad. Por lo tanto, uno de los objetivos de la UE es aprovechar el potencial de los datos sanitarios fuera de la UE, en consonancia con los principios del Espacio Europeo de Datos Sanitarios, que pretenden promover una gobernanza más sólida de los datos sanitarios y una mayor interoperabilidad. Uno de los ejemplos prácticos que contribuye a avanzar hacia este objetivo se refiere al proyecto lanzado por la Oficina Regional de la OMS para Europa y la Comisión Europea, en el marco del Programa UE para la Salud, para fortalecer los sistemas de información sanitaria e impulsar la gobernanza y la interoperabilidad de los datos sanitarios en 53 países de la región europea de la OMS. Este proyecto de cuatro años tiene como objetivo mejorar el uso y la reutilización de los datos de salud por parte de los proveedores de atención médica, los responsables políticos y los pacientes, así como mejorar la calidad y la interoperabilidad de los sistemas de información de salud.

La estrategia destaca los esfuerzos dirigidos a las prioridades sanitarias mundiales críticas, detallando los progresos realizados y la acción en curso de la UE en este ámbito. En

particular, junto con este informe, también se publicó el anexo respectivo, que presenta una lista no exhaustiva de acciones clave para la implementación de la Estrategia de Salud Mundial.

La Comisión seguirá comprometida con el seguimiento de la aplicación del Espacio Europeo de Datos Sanitarios y tendrá hasta marzo de 2027 para adoptar una serie de actos de ejecución clave que establezcan normas detalladas para la puesta en marcha del Reglamento (UE) 2025/327.

Publicado un informe conjunto entre la AEPD y el Supervisor Europeo de Protección de Datos (EDPS) sobre las implicaciones en materia de privacidad del uso de aprendizaje federado en inteligencia artificial

La AEPD y el EDPS han publicado un informe conjunto sobre el aprendizaje federado, una técnica para entrenar modelos de inteligencia artificial. Esta técnica implica que los modelos se entrenan localmente en cada dispositivo y solo se comparte el resultado, sin necesidad de enviar los datos originales a un servidor central, lo que reduce riesgos de filtraciones y accesos indebidos. El informe destaca aplicaciones en el sector sanitario, asistentes de voz y vehículos autónomos.

El informe reafirma que el aprendizaje federado se alinea con principios como la minimización de datos y la limitación de finalidad, además de reforzar la responsabilidad proactiva y la auditabilidad. Sin embargo, advierte que no debe asumirse que los parámetros intercambiados son anónimos sin un análisis técnico y legal, ya que podrían permitir inferencias sobre datos sensibles. También subraya la necesidad de implementar medidas de seguridad en todo el ecosistema, garantizar la calidad y ausencia de sesgos en los datos distribuidos, y proteger el sistema frente a ataques que exploten el eslabón más débil.

El Comité Europeo de Protección de Datos (CEPD) publica la versión definitiva de las Directrices 2/2024 sobre el articulo 48 RGPD

Tras una publicación provisional de las directrices sobre el artículo 48 del RGPD en relación con las transferencias de datos a las autoridades de terceros países, se ha publicado la versión definitiva de las mismas, con algunos cambios respecto de la primera versión.

Las citadas directrices, tal como se explicó en la newsletter del mes de abril, se centran en las solicitudes destinadas a la cooperación directa entre una autoridad pública de un tercer país y una entidad privada de la UE, remarcando la necesidad de que dichas transferencias estén amparadas en una base legitimadora y en uno de los mecanismos previstos en el RGPD para la realización de transferencias internacionales. En la versión definitiva se han añadido algunos matices, entre los cuales vamos a destacar los más relevantes.

Estas directrices no son de aplicación si el requerimiento de transferencia emana de una subsidiaria o matriz del grupo fuera del EEE, aunque esté respaldado por un requerimiento de la autoridad ubicado en dicho país fuera del EEE. Además, refuerza la idea de que, si el requerimiento lo hace la autoridad a un encargado del tratamiento, este deberá informarlo al responsable del tratamiento y seguir sus instrucciones, siempre y cuando la ley no lo prohíba con base en un importante interés público. Por último, también añade que los acuerdos internacionales en los que se ampare la transferencia deberían permitir que las autoridades soliciten información a entidades privadas, y que no se trate de una mera cooperación entre autoridades públicas. En caso de duda de que exista un acuerdo internacional y de su contenido, el CEPD indica que deberá consultarse a las autoridades nacionales (Ministerio de Justicia y Ministerio de Asuntos Exteriores, entre otros).

El Consejo y el Parlamento Europeo llegan a un acuerdo para mejorar el cumplimiento transfronterizo del RGPD en beneficio de la ciudadanía

El Consejo y el Parlamento Europeo han alcanzado un acuerdo provisional acerca de un nuevo acto jurídico (que, previsiblemente, se configurará como un reglamento) para agilizar y armonizar los procedimientos administrativos transfronterizos en materia de protección de datos, aumentando la cooperación entre las autoridades de control y mejorando así la eficiencia en la aplicación del RGPD.

En este sentido, el nuevo reglamento reconoce diversos aspectos entre los que se encuentran la flexibilización de los requisitos para que el reclamante sea oído en los procedimientos de reclamaciones, o la regularización de los plazos para finalizar las investigaciones (15 meses prorrogables a otros 12 meses, salvo los simplificados que deberán cerrarse en 12 meses). Igualmente, se ha acordado un mecanismo de resolución temprana que permita a las autoridades de protección de datos resolver un caso antes de implicar a otras autoridades extranjeras.

Asimismo, se recoge una medida consistente en la obligación de que la autoridad principal envíe un resumen de las cuestiones clave a sus homólogas de la Unión Europea. Por último, se mantiene una propuesta del Consejo relativa a un procedimiento simplificado de cooperación, consistente en la posibilidad de no aplicar la normativa adicional para procedimientos transfronterizos cuando un asunto no suscite excesiva complejidad, disminuyendo así la carga administrativa de las autoridades.

La AEPD analiza si es obligatorio que un sistema de inteligencia artificial que se utiliza en comunicaciones comerciales automatizadas entienda y ejecute políticas de privacidad

La Agencia Española de Protección de Datos (AEPD) estudia un caso en el que una empresa envía comunicaciones comerciales automatizadas a través de un sistema de inteligencia artificial por mensajería instantánea. La persona receptora de los mensajes alega no haber dado su consentimiento y estar inscrita en la lista Robinson, y solicita el cese de los envíos. Sin embargo, la empresa había establecido un procedimiento claro y gratuito para oponerse al tratamiento de datos con fines promocionales que consistía en responder con la palabra "baja". El sistema de IA solo reconocía esa palabra y no estaba programado para interpretar otras formulaciones de oposición. A pesar de las reiteradas respuestas de la persona solicitando la baja, al no emplear el término exacto, el sistema no procesó su solicitud.

La AEPD destaca varios puntos clave:

i. Procedimiento de oposición claro y gratuito: la empresa ofrecía un método sencillo para oponerse al tratamiento de datos (enviar "baja"), cumpliendo así con la normativa de protección de datos.

ii. Limitaciones del sistema de IA: la Agencia considera que, aunque sería deseable que los sistemas de IA pudieran interpretar cualquier formulación humana de oposición, no es exigible legalmente que estén preparados para ello. No se puede requerir que un sistema automatizado entienda todas las posibles formas en que una persona puede ejercer sus derechos.

iii. Información sobre el uso de IA: la AEPD recuerda que, a partir de agosto de 2026, será obligatorio informar expresamente a los usuarios de que están interactuando con un sistema de IA, aunque

actualmente solo lo recomienda como buena práctica.

iv. Disponibilidad de otros canales: se subraya que la persona podía ejercer sus derechos por otros medios, como correo electrónico o web, y que existía atención humana disponible para gestionar estas solicitudes.

En conclusión, la AEPD entiende que la empresa cumplía con la obligación de ofrecer un canal claro y gratuito para ejercer el derecho de oposición, y que no es exigible que el sistema de IA interprete cualquier mensaje. Además, la existencia de canales alternativos para contactar con agentes humanos refuerza la posición de la empresa en cuanto al cumplimiento de la normativa.

La AEPD responde a la consulta previa relativa al uso de biometría para control de accesos en instalaciones de la Guardia Civil

La AEPD ha emitido una respuesta a una consulta previa realizada con base en el artículo 36 del RGPD relativa a la implementación de un sistema de control de accesos mediante biometría en instalaciones de una entidad pública de seguridad.

El sistema propuesto no genera una base de datos centralizada, sino que conserva la plantilla biométrica en poder del usuario, lo que reduce los riesgos de tratamiento masivo. La finalidad del tratamiento es la identificación y control de acceso de personas, vehículos y residentes en instalaciones sensibles, con base legal en diversas normas como la Ley Orgánica 7/2021, la Ley Orgánica 2/1986 y el RGPD.

La AEPD analiza la legitimidad del tratamiento, destacando que los datos biométricos son categorías especiales que requieren garantías reforzadas. Se distingue entre identificación y autenticación, siendo esta última menos intrusiva y más proporcional en contextos controlados. El sistema incorpora medidas técnicas avanzadas como la generación local de identificadores no reversibles, control exclusivo por el interesado, ausencia de almacenamiento centralizado y limitación estricta a fines de autenticación. Estas características permiten minimizar el impacto sobre los derechos fundamentales.

La AEPD concluye que el tratamiento biométrico propuesto cumple con los requisitos de legalidad, necesidad y proporcionalidad, y que no existen alternativas igualmente eficaces con menor impacto. No obstante, recomienda una evaluación diferenciada en zonas con menor criticidad, así como la posibilidad de ofrecer alternativas no biométricas en ciertos casos. Finalmente, se destaca la importancia de realizar evaluaciones de impacto periódicas, garantizar el cumplimiento del Esquema Nacional de Seguridad y mantener la protección de los datos bajo control exclusivo del interesado, evitando su uso indebido o acceso por terceros.

Publicada una guía de la Comisión Europea sobre las obligaciones de los modelos de IA de propósito general

La Comisión Europea ha publicado directrices interpretativas sobre el alcance de las obligaciones aplicables a los proveedores de modelos de inteligencia artificial de propósito general (GPAI) conforme al Reglamento (UE) 2024/1689 (AI Act), cuya aplicación efectiva comienza el 2 de agosto de 2025.

Las directrices de la Comisión Europea sobre el Reglamento de Inteligencia Artificial (AI Act) aclaran las obligaciones que deben cumplir los proveedores de modelos de IA de propósito general, especialmente aquellos con riesgo sistémico. Establecen criterios técnicos (como el cómputo de entrenamiento en FLOP) para identificar estos modelos, detallan las obligaciones de transparencia, documentación, cumplimiento de derechos de autor y evaluación de riesgos, y prevén exenciones para modelos *open-source* bajo condiciones estrictas.

Además, regulan la supervisión por parte de la Oficina de IA, los procedimientos de notificación y clasificación, y el régimen transitorio hasta la plena aplicación del régimen sancionador en agosto de 2026.

El EDPB emite una declaración sobre los términos contractuales tipo no vinculantes del 'Data Act'

El Comité Europeo de Protección de Datos (EDPB) ha emitido una declaración sobre los términos contractuales modelo (MCTs) propuestos por la Comisión Europea para facilitar el intercambio de datos conforme al artículo 41 del *Data Act*.

El EDPB advierte de que estos términos, aunque no vinculantes, deben alinearse con el Reglamento General de Protección de Datos (RGPD) cuando se trate de datos personales. Entre sus observaciones, destaca la necesidad de distinguir claramente entre datos personales y no personales, mejorar la estructura y definiciones de los MCTs, y asegurar que las cláusulas contractuales no prevalezcan sobre la normativa de protección de datos en caso de conflicto.

Asimismo, recuerda que el cumplimiento de los MCTs no garantiza por sí solo la conformidad con el RGPD, y que pueden requerirse medidas adicionales como cláusulas contractuales tipo en transferencias internacionales. También recomienda considerar la vulnerabilidad del consumidor y evitar cláusulas sancionadoras desproporcionadas.

El EDPB se mantiene disponible para seguir colaborando en la mejora de estos instrumentos contractuales.

El CEPD contribuye a la consulta pública de la Autoridad Bancaria Europea (EBA) sobre los proyectos de normas técnicas de regulación (RTS) en materia de prevención de blanqueo de capitales y financiación del terrorismo (AML/CFT)

El CEPD indica que, puesto que los sujetos obligados al cumplimiento de las obligaciones AML/CFT pueden ser personas físicas, ello conlleva el tratamiento de datos personales, por lo que se debería incluir una referencia en las RTS a la aplicabilidad del RGPD.

Asimismo, realiza una serie de apuntes a modificar en la propuesta de RTS, tales como:

i. Incluir una mención expresa a la obligación de contar con medidas técnicas y organizativas adecuadas en virtud del artículo 32 RGPD.

ii. En relación con la verificación remota de identidad, el tratamiento de los datos personales no debería basarse en el consentimiento, ya que no es opcional para el cliente proporcionar esta información, por lo que la AEPD sugiere que la base legal sea el cumplimiento de una obligación legal (artículo 6.1.c) RGPD).

iii. Clarificar que la información almacenada debe ser actualizada y rectificada sin retraso indebido.

iv. Asegurar que se cumple con el principio de minimización en cuanto a la recopilación de datos personales de terceros en caso de sospecha de actividad delictiva.

La AEPD y la Autoridad de protección de datos de Brasil amplían su colaboración institucional

En el marco de la *Global Privacy Assembly* (GPA) celebrada en Seúl, el presidente de la Agencia Española de Protección de Datos

(Lorenzo Cotino) y el director-presidente de la Autoridad Nacional de Protección de Datos de Brasil (Waldemar Gonçalves) han firmado la renovación del Memorando de Entendimiento (MOU) entre ambas instituciones. Este acuerdo refuerza la colaboración institucional y establece un marco para el desarrollo de acciones conjuntas orientadas a la promoción y aplicación práctica de la protección de datos personales.

El MOU contempla el intercambio de conocimientos técnicos, la cooperación en investigaciones, estudios y análisis, así como la elaboración de guías y herramientas para facilitar el cumplimiento normativo. Además, se prevé el desarrollo de iniciativas conjuntas, especialmente en el contexto de programas y proyectos internacionales.

En el ámbito iberoamericano, destaca la labor conjunta en la Red Iberoamericana de Protección de Datos, foro presidido actualmente por la ANPD y con la Agencia Española como secretaría permanente. Entre los logros recientes figura la aprobación de los "Estándares Iberoamericanos de Protección de Datos", que promueven la adopción de mecanismos para el intercambio de mejores prácticas y experiencias entre los Estados de la región.

Este acuerdo consolida la cooperación internacional y el liderazgo de ambas autoridades en la protección de datos personales a nivel global e iberoamericano.

Investigadores del 'Joint Research Centre' de la Comisión Europea publican un artículo sobre 'AI Benchmarks'

En el artículo se analizan los problemas y limitaciones de los *benchmarks* o indicadores de referencia en inteligencia artificial (IA), los cuales se han convertido en herramientas clave para evaluar el rendimiento, capacidades y riesgos de los sistemas de IA, y son cada vez más relevantes tanto para la investigación como para la regulación, especialmente en el contexto de la aplicación del *European AI Act*. En este sentido, el estudio parte de la premisa de que, aunque los *benchmarks* permiten comparar modelos y medir avances, su uso generalizado ha suscitado preocupaciones sobre su idoneidad para evaluar aspectos sensibles como la seguridad, el impacto social o los riesgos sistémicos de la IA.

El artículo concluye que los *benchmarks* actuales, en su mayoría cuantitativos y orientados al rendimiento, no son suficientes para proporcionar las garantías de seguridad y fiabilidad que exigen los legisladores y la sociedad. Por ello, los autores recomiendan exigir mayor transparencia y documentación en la creación y uso de *benchmarks*, promover la diversidad e inclusividad en su diseño, desarrollar *benchmarks* dinámicos y multimodales que reflejen mejor los riesgos y capacidades reales de los sistemas de IA, y establecer protocolos rigurosos de validación y actualización.

Además, abogan por evaluar no solo el rendimiento, sino también los errores, fragilidades y consecuencias no deseadas de los modelos, y por crear mecanismos para valorar la fiabilidad de los propios *benchmarks*, más allá de su popularidad o número de citas.

La 'Information Commissioner's Office' (ICO) del Reino Unido publica un artículo sobre cómo garantizar la anonimización efectiva de datos personales

El artículo proporciona una guía para la anonimización efectiva de datos personales, ofreciendo un enfoque práctico y estratégico para garantizar que este proceso se lleve a cabo de forma efectiva, permitiendo a las entidades tratar datos sin comprometer la privacidad de los usuarios.

Así pues, para evaluar si un conjunto de datos ha sido anonimizado de forma efectiva, la ICO propone aplicar el llamado *"motivated intruder test"*. Esta prueba consiste en analizar si una persona con motivación, conocimientos y recursos razonables podría identificar a un usuario utilizando los datos anonimizados

junto con información disponible públicamente. Si existe una probabilidad significativa de identificación, los datos no pueden considerarse anónimos.

Además, la guía enfatiza que la anonimización debe ser efectiva no solo para el responsable del tratamiento, sino también para cualquier tercero que tenga acceso a los datos. Igualmente, la ICO recomienda que las organizaciones adopten un enfoque estratégico y técnico proponiendo la realización de evaluaciones de impacto en la protección de datos (DPIA) cuando sea necesario, y documentar cuidadosamente las decisiones y medidas adoptadas. La guía proporciona pasos prácticos para identificar riesgos, aplicar técnicas de anonimización adecuadas y establecer controles que refuercen la protección de la información.

Finalmente, el artículo concluye resaltando los múltiples beneficios que ofrece la implementación de las medidas expuestas, que permiten compartir y reutilizar datos con menos restricciones legales, fomentar la innovación responsable y mejorar la transparencia ante los interesados. Además, reduce la carga regulatoria al excluir los datos anonimizados del ámbito del UK GDPR, lo que, según la ICO, podría facilitar proyectos de análisis, investigación y desarrollo tecnológico.

Alejandro Padín
Socio · Madrid
alejandro.padin@garrigues.com

Luisa Cyrne
Asociada principal · Lisboa
luisa.cyrne@garrigues.com

Adrián León
Asociado · Alicante
adrian.leon@garrigues.com

Garazi Tomás
Asociada · Bilbao
garazi.tomas@garrigues.com

Javier Enebral
Asociado · Madrid
javier.enebral@garrigues.com

Marta Sabio
Asociada · Barcelona
marta.sabio@garrigues.com

Manuel Liberal Jerónimo
Socio · Lisboa y Oporto
manuel.liberal.jeronimo@garrigues.com

Sebastián Hassi
Asociado principal · Santiago de Chile
sebastian.hassi@garrigues.com

Antonio Durán
Asociado · Málaga
antonio.duran@garrigues.com

Ignacio Suárez
Asociado · Madrid
ignacio.suarez@garrigues.com

Laia Llambric
Asociada · Bilbao
laia.llambrich@garrigues.com

Matilde Bettencourt
Asociada · Lisboa
matilde.bettencourt@garrigues.com

Más información:

Economía del Dato, Privacidad y Ciberseguridad

GARRIGUES

Plaza de Colón, 2
28046 Madrid
T +34 91 514 52 00
info@garrigues.com

Síguenos en:

Esta publicación contiene información de carácter general, sin que constituya opinión profesional ni asesoramiento jurídico.

© **J&A Garrigues, S.L.P.**, quedan reservados todos los derechos. Se prohíbe la explotación, reproducción, distribución, comunicación pública y transformación, total y parcial, de esta obra, sin autorización escrita de J&A Garrigues, S.L.P.