DURÁNSINDREU

Newsletter
Protección de datos

ABRIL 2025

En este nuevo número de la Newsletter de protección de datos de abril 2025, se detallan las novedades introducidas por la aprobación por parte del Gobierno del *Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial*, adaptando la legislación española al Reglamento (UE) 2024/1689 relativo a normas armonizadas en materia de Inteligencia Artificial (RIA). Esta normativa establece prohibiciones claras a prácticas manipulativas basadas en IA, impone obligaciones para sistemas de alto riesgo y establece requisitos de transparencia y supervisión, con sanciones que pueden alcanzar los 35 millones de euros.

En materia de resoluciones de la AEPD, se destacan tres resoluciones en las que la AEPD establece: una multa de 500.000€ a una concesionaria sanitaria por no comunicar el uso de subencargados de tratamiento; una sanción a una empresa por no garantizar la seguridad efectiva de datos personales pese a contar con políticas; y una sanción 70.000€ a una empresa logística por entregar un paquete con datos personales a un destinatario no autorizado.

Finalmente, se hace mención a la reafirmación por parte de la AEPD de su postura sobre el tratamiento del DNI con una multa de 8.000€ a una empresa por fotografiar un DNI con un móvil personal, no informar sobre el tratamiento y carecer de carteles de videovigilancia, subrayando la importancia del principio de minimización.

Novedades destacables

El Gobierno aprueba el Anteproyecto de Ley de IA

El pasado 11 de marzo de 2025, el Consejo de Ministros aprobó el anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial, que adapta la legislación española al Reglamento (UE) 2024/1689 de Inteligencia Artificial.

Su objetivo es garantizar un uso ético, inclusivo y seguro de la IA, estableciendo un régimen sancionador claro y medidas de supervisión. Entender las implicaciones legales de este Anteproyecto es clave para todas aquellas entidades que hagan uso de herramientas con Inteligencia Artificial.

Los puntos clave del anteproyecto se pueden dividir en tres:

- Prohibiciones claras: Desde el 2 de febrero de 2025, se prohíben prácticas como técnicas subliminales para manipular, explotación de vulnerabilidades por edad o discapacidad, y clasificación biométrica por raza u orientación sexual. Las sanciones, aplicables desde el 2 de agosto de 2025, pueden llegar a 35 millones de euros o el 7% del volumen de negocio mundial, con ajustes para pequeñas y medianas empresas (PYMES).
- Obligaciones para sistemas de alto riesgo: Sistemas como los usados en biometría, infraestructura crítica, educación, empleo, justicia y migración deben cumplir con medidas como gestión de riesgos, supervisión humana y gobernanza de datos. Las infracciones

graves, como no reportar incidentes severos, pueden acarrear multas de hasta 15 millones de euros o el 3% del volumen de negocio.

- Transparencia: Los proveedores de sistemas de IA tendrán la obligación de etiquetar correctamente cualquier imagen, vídeo o audio generado o manipulado con IA que constituya una suplantación (*deepfake*) o cualquier texto destinado a informar al público sobre asuntos de interés público, así como el deber de informar a las personas afectadas sobre el hecho de que están interactuando con un sistema de IA.
- Supervisión: La Agencia Española de Supervisión de IA y otras autoridades sectoriales (AEPD, CGPJ, JEC) vigilarán el cumplimiento, con posibilidad de aplicar medidas cautelares como la retirada temporal de sistemas de IA.

Este anteproyecto es especialmente relevante para empresas en sectores como **banca, salud y educación**, que deben prepararse para **cumplir con las nuevas obligaciones** y evitar sanciones significativas. Al alinearse con la normativa europea, también facilita la operatividad internacional de las empresas.

Se debe tener en cuenta que todavía se debe seguir un proceso para la aprobación definitiva de esta normativa. El Anteproyecto se tramitará por la vía de urgencia y deberá pasar por las Cortes Generales del Estado para su debida tramitación parlamentaria.

Resoluciones de la AEPD

Concesionaria sanitaria sancionada por la AEPD: incumplimiento del deber de comunicación del uso de subencargados del tratamiento

La AEPD ha impuesto una **multa de 500.000** euros a una entidad concesionaria de un Departamento de Salud, por vulnerar el artículo 28.2 del RGPD.

Desde 2009, la entidad gestionaba el Departamento de Salud de un municipio por concesión. Durante la fase final del contrato, que no fue renovado y expiró en enero de 2024, la Conselleria de Sanidad detectó falta de transparencia en la subcontratación de servicios con acceso a datos especialmente protegidos, como datos de salud o datos genéticos.

¿Qué ocurrió para que se aplicara una sanción de este importe?

- La entidad **no informó adecuadamente** al Responsable del tratamiento sobre los subencargados de tratamiento de datos personales.
- Pese a contar con una autorización general desde 2009, el RGPD exige **informar previamente** de cualquier cambio en los subcontratistas al responsable del tratamiento, en este caso, la Conselleria.
- La AEPD determinó que la **falta de notificación** violaba el principio de responsabilidad proactiva.

¿Por qué es relevante?

- El tratamiento implicaba **datos de especial sensibilidad**.
- La multa, aunque significativa, representa solo el 0,3% del volumen de negocio de la entidad en 2022.
- Marca un **precedente importante** en el ámbito sanitario sobre las obligaciones del encargado de tratamiento.

En conclusión, este caso subraya la necesidad de cumplir **con todas las obligaciones del RGPD**, especialmente en sectores sensibles como el sanitario. Informar al responsable del tratamiento sobre los subencargados no es opcional, y su omisión puede conllevar importantes sanciones.

Empresa sancionada por la AEPD: incumplimiento del deber de garantizar la seguridad de los datos

La AEPD reafirma la importancia de **contar con unas políticas de tratamiento de datos personales efectivas y verificables**. En este caso, el empleado de una empresa compartió datos personales de sus clientes a terceras personas no autorizadas sin el consentimiento de los interesados. Aunque la empresa disponía de políticas internas, formación y un sistema de trazabilidad de accesos, la AEPD determinó que estas medidas eran insuficientes, siendo la empresa incapaz de demostrar que había implementado controles efectivos para prevenir accesos no autorizados ni garantizar el cumplimiento de sus propias normas.

Además, la AEPD considera que las medidas de seguridad que la empresa había incorporado en sus políticas **no se estaban implantando en la práctica**, concluyendo que no es suficiente con que el responsable del tratamiento implante medidas de seguridad, sino que también, debe asegurar su cumplimiento.

De esta resolución se pueden extraer las **siguientes conclusiones:**

- **Políticas de seguridad efectivas:** Para cumplir con las obligaciones legales en materia de protección de datos no es suficiente con contar con las políticas y procedimientos exigibles legalmente. Es importante que las medidas técnicas y organizativas presentes en dichas políticas se cumplan debidamente por parte de la empresa y que sean suficientes para mitigar o reducir los riesgos frente a accesos no autorizados o divulgaciones ilícitas.
- **Principio de responsabilidad proactiva:** Las empresas no sólo deben cumplir con la normativa, sino que deben ser capaces de documentarlo. Es por ello por lo que son muy importantes los registros internos y la documentación de todas las medidas implantadas en materia de protección de datos. La mera aprobación de una política de privacidad no asegura el cumplimiento normativo.

Esta resolución de la AEPD no solo reafirma la importancia de una gestión rigurosa de los datos personales, sino que también envía un mensaje claro: las empresas **deben anticiparse a los riesgos** y **demostrar** que sus medidas de seguridad funcionan, o enfrentarán sanciones severas.

Empresa logística sancionada por la AEPD: entrega indebida y vulneración del principio de confidencialidad

La AEPD ha impuesto una sanción de 70.000 euros a una empresa por infringir el artículo 5.1.f) del Reglamento General de Protección de Datos (RGPD), relativo al principio de integridad y

confidencialidad como consecuencia de una entrega indebida de un paquete que expuso datos personales a un tercero no autorizado, evidenciando los riesgos en la gestión de datos en servicios logísticos.

¿Qué ocurrió en este caso?

- **Entrega indebida de un paquete**: La empresa entregó un paquete a una persona no autorizada en una dirección incorrecta, incumpliendo su protocolo interno, que requería verificar la identidad del destinatario, en este caso, el titular de un contrato específico.
- **Exposición de datos personales**: La etiqueta del paquete contenía datos sensibles del reclamante (nombre, apellidos, dirección y número de teléfono), que quedaron accesibles a un tercero, vulnerando el principio de confidencialidad.
- **Falta de diligencia**: Aunque existían medidas internas, la empresa no aseguró su correcta aplicación, lo que facilitó la brecha de datos, sin evidencia de intencionalidad, pero con negligencia en la ejecución del proceso de entrega.

¿Por qué es relevante?

- **Importancia de la ejecución efectiva**: La resolución subraya que no es suficiente con establecer medidas de seguridad; estas deben aplicarse rigurosamente. Esto confirma la necesidad observada en la anterior resolución no sólo de contar con medidas de seguridad sino también de que dichas medidas se respeten y sean suficientes para prevenir brechas de seguridad.
- **Precedente normativo**: La sanción refuerza que el principio de confidencialidad es innegociable y que su incumplimiento, aunque sea en un incidente aislado, puede generar multas relevantes, especialmente para empresas que tratan datos de forma habitual.

Conclusión

Esta resolución evidencia que el cumplimiento del RGPD requiere no solo diseñar políticas, sino garantizar su implementación práctica en cada operación. Las empresas que manejan datos personales, particularmente en logística, deben priorizar la formación, la supervisión y la mejora continua de sus procesos para evitar sanciones y proteger la confianza de sus clientes. La lección es clara: la diligencia en la protección de datos es una obligación ineludible.

La AEPD refuerza su postura sobre el tratamiento del DNI

En ediciones anteriores de esta *Newsletter*, destacamos cómo la AEPD ha **intensificado su vigilancia sobre el uso del Documento Nacional de Identidad**, subrayando su carácter especialmente sensible y recordando que solo debe tratarse cuando exista una base legal clara que lo justifique.

Este mes, retomamos esta cuestión a raíz de una nueva resolución que ilustra cómo prácticas aparentemente rutinarias —como fotografiar un DNI con un teléfono móvil particular— pueden **derivar en sanciones relevantes** cuando no se respetan los requisitos del RGPD. La resolución refuerza, una vez más, la importancia de tratar este tipo de datos con el máximo nivel de precaución y de garantizar que los procedimientos internos estén alineados con la normativa vigente.

Sanción de 8.000€ a una empresa por varias vulneraciones del RGPD relativas al tratamiento de datos personales contenidos en el DNI de un usuario.

La AEPD ha sancionado a una entidad con una multa total de 8.000€ por **cuatro infracciones** del RGPD relacionadas con el tratamiento inadecuado de datos personales.

¿Qué ocurrió?

En marzo de 2024, un cliente denunció que, para recoger su vehículo, se le exigió mostrar el DNI, cuya imagen fue fotografiada con el móvil personal de un empleado, sin recibir ninguna información sobre el tratamiento de sus datos. Además, el local contaba con cámaras de seguridad sin carteles informativos de videovigilancia.

Infracciones detectadas:

1. **Vulneración del principio de minimización de datos** (art. 5.1.c RGPD): se consideró que la finalidad perseguida —demostrar que el usuario era el autorizado para retirar el vehículo— podía haberse cumplido de manera menos intrusiva, como mediante la mera exhibición del documento.
2. **Falta de medidas de seguridad** (art. 32 RGPD): el uso de un móvil personal para la captación del DNI de un cliente evidencia deficiencias en medidas técnicas y organizativas en el tratamiento de datos personales.
3. **Incumplimiento del deber de información** (art. 13 RGPD): el cliente no fue informado de cómo se tratarían sus datos.
4. **Ausencia de carteles de videovigilancia** (art. 13 RGPD): la AEPD también observó que las instalaciones de Grúas Ignaci contaban con un sistema de videovigilancia que carecía de la cartelería informativa exigida por la normativa. El hecho de no informar mediante señales visibles sobre la existencia de cámaras y el tratamiento de las imágenes también constituye una infracción del RGPD, especialmente cuando afecta potencialmente a cualquier persona que acceda al establecimiento

Como resultado del procedimiento sancionador, la empresa fue sancionada con **tres multas** diferenciadas:

- 3.000€ por la recogida excesiva de datos (DNI).
- 2.000€ por la falta de seguridad en el tratamiento.
- 3.000€ por la ausencia de información y señalización de videovigilancia.

Medidas correctivas impuestas:

Además de la sanción económica, la resolución de la AEPD impone a la entidad infractora la obligación de adoptar diversas medidas correctivas en un plazo de dos meses. Entre ellas:

- Evitar captación de imágenes del DN.
- Implantar medidas de seguridad en el tratamiento de datos.
- Informar adecuadamente a los usuarios.
- Colocar los carteles de videovigilancia en zonas visibles.

Conclusión

Este caso subraya la importancia de **aplicar el principio de minimización de datos**, establecer medidas de seguridad efectivas, y cumplir con el deber de informar. Pequeñas empresas también están obligadas a respetar el RGPD, y su incumplimiento puede acarrear sanciones económicas y reputacionales.

Contacto

Carme Setó
Socia | IP&IT y protección de datos
cseto@duransindreu.com
93 602 52 22

Cristina Miñana
Abogada | IP&IT y protección de datos
cminyana@duransindreu.com
93 602 52 22

Iván Roda
Abogado | IP&IT y protección de datos
iroda@duransindreu.com
93 602 52 22

Bàrbara Boguñá
Abogada | IP&IT y protección de datos
bboguna@duransindreu.com
93 602 52 22

Pere Puig
Área de IP&IT y protección de datos
ppuig@duransindreu.com
93 602 52 22