DURÁNSINDREU

Newsletter
Protección de datos

DICIEMBRE 2024

Esta newsletter presenta una recopilación práctica de novedades clave en el ámbito de la protección de datos. Comenzamos con un análisis detallado de la Entrada en vigor de la Directiva NIS2, destacando su impacto en distintos sectores económicos y las nuevas obligaciones de ciberseguridad impuestas. En el segmento de Protección de Datos, se exploran diferentes aspectos a través de la Opinión 22/2024 del Comité Europeo de Protección de Datos sobre encargados y subencargados, así como las Directrices 1/2024 relativas al uso del "interés legítimo" como base jurídica de tratamiento. Además, se revisa el primer informe del CEPD sobre el Marco de Privacidad de Datos entre la UE y EE. UU. También se incluyen resoluciones recientes de la AEPD, como sanciones impuestas a una entidad de telecomunicaciones por fallos de seguridad, y una entidad bancaria por la eliminación indebida de datos personales. Finalmente, se destacan sentencias importantes del Tribunal de Justicia de la Unión Europea y del Tribunal Supremo, relevantes para el tratamiento y protección de datos en el marco de la normativa vigente de la UE.

Novedad destacable

Entrada en vigor de la NIS2

El pasado 17 de octubre de 2024 finalizó el plazo para la transposición de la Directiva 2022/2555, conocida como NIS2, la cual es una actualización de Directiva NIS original (adoptada en 2016) y tiene como objetivo mejorar la ciberseguridad en el espacio europeo.

Principales novedades que conlleva la Directiva

- Ampliación del ámbito de aplicación a sectores tales cómo sanitario, servicios digitales o producción, transformación y distribución de alimentos.

- Establecimiento de nuevas obligaciones. Las entidades de los sectores afectados deberán cumplir con la obligación de **gestión de riesgos de ciberseguridad**, consistente en un listado **mínimo** de medidas técnicas, operativas y de organización. Asimismo, la directiva establece **la obligación de notificar** cualquier **incidente significativo.**

- **Endurecimiento de las sanciones** ante el incumplimiento, las cuales pueden suponer multas con un máximo de al menos 7.000.000€ o 10.000.000€; o hasta el 1,4% o 2% del volumen de negocios total anual, optándose por la de mayor cuantía, en función del caso.

Para más información si tu entidad pertenece a un sector sujeto a la aplicación de la NIS2 consulta el siguiente enlace: https://www.incibe.es/incibe-cert/sectores-estrategicos/FAQNIS2

Novedades en Protección de Datos

Opinión 22/2024 CEPD: Obligaciones de encargados y subencargados

El Comité Europeo de Protección de Datos (CEPD) publicó el pasado 7 de octubre la Opinión 22/2024, mediante la que detalla determinados aspectos de la relación entre los Responsables y Encargados y Subencargados del Tratamiento de datis.

Aspectos destacables:

- Necesidad de identificar los **encargados y subencargados** que intervengan en cualquier fase del tratamiento de los datos.
- Importancia de que el encargado imponga en el subencargado **las mismas obligaciones** de protección de datos establecidas en el contrato inicial entre el responsable y el encargado.
- Supervisión constante: el encargado principal debe monitorizar de forma continuada a los subencargados.
- Facultad del Responsable del Tratamiento a autorizar, o no, el uso de subencargados ya sea mediante una autorización específica o general.
- **Responsabilidad compartida**: los incumplimientos de un subencargado podrían generar responsabilidades para el encargado principal.

Para ello, resulta necesario que **las entidades auditen la relación contractual con sus encargados y subencargados** a los efectos de adecuarlos a las necesidades de control y supervisión indicados.

Directrices 1/2024: tratamiento de datos en base al interés legítimo

El CEPD adoptó, el pasado 9 de octubre, las Directrices 1/2024 sobre el tratamiento de datos personales basado en el artículo 6.1.f) del RGPD, que **establece el "interés legítimo" como una de las bases legitimadoras**. Estas Directrices tienen como objetivo **principal proporcionar unos criterios** a seguir en el uso del interés legítimo cómo base jurídica para el tratamiento de datos personales.

Metodología para la evaluación del interés legítimo

Para poder basar el tratamiento de datos en el interés legítimo deben concurrir tres presupuestos:

1) El Responsable o un tercero deben perseguir un interés legítimo y específico.
2) El tratamiento de datos debe ser estrictamente el necesario para alcanzar el interés legítimo identificado.
3) Los derechos fundamentales del interesado no prevalecen sobre el interés legítimo del Responsable o del tercero.

Por lo que, la identificación de un interés legítimo **no es suficiente** para que sea considerada una base jurídica adecuada para el tratamiento de los datos con base al artículo 6.1.f) del RGPD. Resulta necesario la concurrencia de los presupuestos indicados para que prospere un tratamiento de datos bajo la indicada base jurídica.

Asimismo, el CEPD recuerda la **obligatoriedad de informar de manera clara y detallada a los interesados** sobre el uso de esta base jurídica.

Para ello, el uso del interés legítimo como base jurídica válida en un tratamiento de **datos requiere de una ponderación y análisis pormenorizado** de acuerdo con la normativa vigente.

El CEPD publica un primer informe en relación con el Marco de Privacidad de datos entre UE-EE. UU.

El CEPD ha adoptado recientemente un informe inicial sobre la implementación del Marco de Privacidad de Datos UE – EE. UU., el cual supone una herramienta clave para la transferencia internacional de datos entre la Unión Europea y Estados Unidos, tras la decisión de adecuación de julio de 2023. Así, el informe destaca:

- **Progresos en certificación y sensibilización**: el departamento de Comercio de EE. UU. ha adoptado una serie de medidas para aplicar el proceso de certificación consistentes en el desarrollo de un nuevo sitio web, la actualización de sus procedimientos, y la colaboración con empresas. Además, se ha puesto en marcha un sistema de resolución de reclamaciones.
- **Recursos y Supervisión**: aunque se ha establecido un mecanismo de recurso para los ciudadanos, existe un número bajo de denuncias, por lo que el CEPD insta a EE. UU. a reforzar la supervisión para garantizar que las empresas certificadas cumplan con los principios del Marco de Privacidad de Datos. Asimismo, destaca la importancia de proporcionar orientaciones específicas sobre las obligaciones de las empresas al transferir datos personales desde la UE, así como sobre el tratamiento de datos de recursos humanos.
- **Acceso por parte de autoridades**: el CEPD valora las salvaguardias introducidas en el Decreto nº. 14086, como el principio de proporcionalidad, pero pide a la Comisión Europea monitorear su aplicación y futuros cambios legislativos, como la Sección 702 de la Ley de Vigilancia de Inteligencia Extranjera.

Resoluciones AEPD

Entidad de telefonía móvil sancionada por la AEPD: un recordatorio sobre la responsabilidad en protección de datos

La AEPD ha confirmado la **sanción de 6,5 millones de euros** impuesta en fecha de 27 de diciembre de 2023 contra una **entidad de telefonía móvil tras desestimar el recurso de reposición interpuesto por la mencionada entidad**. La sanción responde a deficiencias graves en la protección de datos personales que permitieron un ciberataque masivo en 2021, el cual afecto a 13 millones de personas.

Contexto:

La brecha de seguridad ocurrida en abril de 2021 permitió a los hackers acceder y publicar datos personales como nombres, direcciones e información bancaria de empleados en la Deep Web. Así, se detectó que la entidad almacenaba dicha información sin cifrado, pseudonimización, ni otras medidas de seguridad.

Resolución de la AEPD: A pesar de los argumentos de la empresa centrados en que la misma había sido víctima de un ataque sofisticado y que tenía implementadas medidas de seguridad adecuadas, **la AEPD desestimó el recurso** y señalo que:

- No constaban implementadas medidas proporcionales al riesgo, pese haber identificado previamente debilidades en una evaluación de impacto de 2018.
- Existieron deficiencias específicas en la política de contraseñas, formación del personal y en la seguridad perimetral y monitorización de los sistemas.
- La cantidad de personas afectadas y la sensibilidad de los datos fueron elementos decisivos en la agravación de la infracción.

Sanción:

- **4 millones de euros** por la infracción del artículo 5.1f) del RGPD, relativo a la confidencialidad e integridad de los datos
- **2,5 millones de euros** por la infracción del artículo 32, que exige la adopción de medidas de seguridad adecuadas.

Entidad bancaria sancionada por la AEPD: eliminación indebida de datos personales

La Agencia Española de Protección de Datos (AEPD) ha impuesto **una sanción de 200.000€ a una entidad bancaria por la vulneración de la normativa de protección de datos personales** en relación con el tratamiento indebido de los datos contenidos en un teléfono móvil corporativo, el cual fue adquirido, al finalizar la relación laboral, por una exempleada.

Elementos del caso:

- **Origen**: una extrabajadora interpuso una reclamación ante la AEPD debido a que, tras adquirir un dispositivo móvil corporativo para su uso personal, el banco eliminó de forma remota toda la información en él contenida, incluyendo datos personales, sin base legitimadora que amparara dicho tratamiento.
- **Normativa vulnerada:** Artículo 6.1 RGPD, el cual exige una base legal para todo tratamiento de datos personales.
- **Calificación**: Infracción muy grave según lo establecido en el art. 83.5 a) RGPD
- **Sanción**: sanción de 200.000€, la cual fue reducida a 120.000€ por el pago voluntario de la entidad.

Sentencias del TJUE

La autoridad de control no está siempre obligada a imponer sanciones

El Tribunal de Justicia de la Unión Europea ha aclarado, en el Asunto C-768/21 de 26 de septiembre de 2024, que las autoridades de control no están obligadas a adoptar medidas correctoras, como multas, en todos supuestos de infracción del Reglamento General de Protección de Datos (RGPD).

Lo anterior resulta especialmente de aplicación cuando el Responsable del tratamiento ya ha tomado las medidas necesarias de manera proactiva para corregir la situación y prevenir futuros incidentes.

Caso destacado en Alemania

Una caja de ahorros detectó que una de sus empleadas había accedido sin autorización a los datos personales de un cliente. A pesar de que la entidad no notificó al cliente, la entidad:

- Tomó medidas disciplinarias contra la empleada
- Garantizó que los datos no habían sido copiados ni compartidos
- Notificó la infracción a la autoridad de protección de datos competente.

Ante lo anterior, la autoridad concluyó que no era necesario adoptar medidas correctivas debido a la actuación proactiva de la entidad.

Puntos clave de la sentencia:

1. La autoridad de control tiene un margen de apreciación para decidir si imponer sanciones es adecuado.
2. No es obligatorio imponer multas si el responsable del tratamiento ha corregido la infracción y tomado medidas preventivas.
3. Ante una brecha de seguridad es importante actuar con rapidez y tomar medidas correctivas efectivas.

Sentencias del Tribunal Supremo (TS)

El Tribunal Supremo anula la sanción de 5 millones de euros impuesta a una entidad bancaria por la AEPD

El pasado 11 de noviembre de 2024, el Tribunal Supremo dictó su sentencia 1792/2024, mediante la que estableció una importante jurisprudencia en el ámbito de la protección de datos y el derecho administrativo sancionador.

Contexto:

La AEPD estableció una **sanción de 5 millones de euros a una entidad bancaria tras haber recibido 5 reclamaciones de interesados independientes**. Así, la sanción se fundamentaba en supuestas infracciones del RGPD derivadas de la política de privacidad del banco y del uso de su formulario de consentimiento.

Resolución del TS:

La resolución dictada por la AEPD fue recurrida y el asunto terminó en manos de la Sala de lo Contencioso-Administrativo del Supremo, la cual anuló la sanción en base a:

- La AEPD se había excedido en sus competencias al transformar unas reclamaciones concretas en una revisión general de la política de privacidad de la entidad.

- Los principios de tipicidad y seguridad jurídicas no fueron respetados, tal y como es requerido en todo procedimiento sancionador
- El hecho de que hubiesen sido presentadas cinco reclamaciones no podía justificar una causa general contra la entidad, más si tenemos en consideración que la misma cuenta con más de 8 millones de clientes.
- La AEPD no puede derivar de reclamaciones concretas una causa general para juzgar la política de privacidad de una entidad sin antes acreditar de forma suficiente la conexión entre las denuncias y las infracciones alegadas.

De ese modo, el Supremo concluyó **que la actuación de la AEPD debía verse limitada a los hechos denunciados** o, en su caso, iniciar un procedimiento independiente con las garantías adecuadas.

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