
ECIJA

NOTA INFORMATIVA

# Incompatibilidades y conflicto de intereses entre el DPD y el RSII según el criterio de la AEPD

La AEPD analiza una brecha de seguridad detectada en el SPEIS de la Diputación Provincial de Huesca y revisa la solidez de su modelo de cumplimiento. En esta resolución, la Agencia evalúa tanto la eficacia de las medidas preventivas como la forma en que se han distribuido responsabilidades internas, especialmente aquellas vinculadas al Delegado de Protección de Datos. El caso aporta claves prácticas para reforzar la gobernanza y garantizar estructuras que aseguren independencia y coherencia en la gestión de datos personales.

## Puntos clave

- La AEPD confirma que la brecha de seguridad en el SPEIS se originó por la falta de controles técnicos y organizativos capaces de evitar el acceso indebido a datos personales, incluidos datos especialmente sensibles.

- Anque la Diputación reaccionó de forma diligente tras el incidente, las actuaciones fueron reactivas y no impiden apreciar la infracción del artículo 5.1.f) RGPD, dado que el acceso no autorizado ya se había producido.

- La resolución destaca la incompatibilidad entre las funciones del Delegado de Protección de Datos y las del Responsable del Sistema Interno de Información de la Ley 2/2023, ya que este último asume tareas operativas que inciden directamente en los fines y medios del tratamiento.

- La DPD de la Diputación planteó ante la AEPD una consulta previa sobre la posible incompatibilidad, que fue resuelta concluyendo que no era posible asignar funciones de responsable del sistema interno de información al DPD en este caso.

- La confusión de ambos papeles debilita las garantías del canal y desnaturaliza la función de protección de datos.

## 1. Resumen de la resolución e infracciones del RGPD apreciadas por la AEPD

La resolución del procedicmiento sancionador recaída en el Expediente con número EXP202316729[1] tramitado por la Agencia Española de Protección de Datos (AEPD) pone el foco en dos aspectos fundamentales que resultan especialmente relevantes desde la perspectiva del cumplimiento normativo. Por un lado, la brecha de seguridad que expuso datos personales y, por otro lado, la existencia de un conflicto de intereses en la estructura de gobernanza de la Diputación, derivado de la acumulación de funciones del Delegado de Protección de Datos (en adelante, "DPD"):

- Brecha de seguridad e infracción del artículo 5.1.f) RGPD. La AEPD considera acreditado que la brecha se originó porque la Diputación no había implementado previamente controles técnicos y organizativos suficientes para evitar el acceso indebido a la carpeta del SPEIS. La configuración de permisos permitió que trabajadores de distintos parques de bomberos accedieran y descargaran documentos cuyo uso debía estar limitado al personal administrativo y directivo del servicio.

  La Agencia opina que con las medidas adecuadas, la brecha "no se habría producido", por lo que la falta de medidas preventivas constituye una vulneración directa del artículo 5.1.f) RGPD. Si bien la Diputación reaccionó con rapidez una vez detectado el incidente bloqueando accesos, iniciando análisis internos, notificando a la AEPD y a los afectados, estas acciones tuvieron carácter reactivo y no evitan la existencia de la infracción, ya que el acceso no autorizado ya se había producido.

- Conflicto de intereses e infracción del artículo 38 RGPD. El aspecto más relevante de la resolución es la apreciación de un conflicto de intereses en la figura del Delegado de Protección de Datos. La Diputación había designado a su DPD también como Responsable del Sistema Interno de Información (RSII), un rol que implica gestionar denuncias internas, tomar decisiones operativas sobre su tramitación y acceder a los datos personales tratados durante la tramitación del expedientes, funciones que inciden directamente en los fines y medios del tratamiento y que resultan incompatibles con la supervisión independiente que exige el artículo 38 RGPD.

  La Agencia destaca que la propia Delegada advirtió sobre la posible incompatibilidad, lo que motivó que la Diputación consultara formalmente a la AEPD. Sin embargo, la Diputación mantuvo el doble rol hasta después del incio del procedimiento, sin realizar un análisis previo de riesgos que garantizase la ausencia de conflicto de intereses.

## 2. Conflicto de intereses entre los roles

Tras exponer los elementos generales de la resolución, resulta conveniente analizar cómo la AEPD evalúa la independencia del DPD cuando sus funciones se relacionan con el Sistema Interno de Información (en adelante, "SII") previsto en la Ley 2/2023 , de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Concretamente, la Agencia examina de qué manera determinadas tareas operativas pueden incidir en la autonomía exigida por el RGPD y qué criterios resultan relevantes para identificar posibles conflictos de intereses conforme al artículo 38 de dicha norma.

[1] El texto completo de la resolución puede consultarse en el siguiente enlace: https://www.aepd.es/documento/ps-00548-2024.pdf

Los puntos clave del razonamiento jurídico de la AEPD para apreciar este conflicto de intereses son los siguientes:

a) Examen funcional, no nominal. La AEPD insiste en que la compatibilidad debe evaluarse atendiendo a las funciones reales, no al título formal del cargo. En este caso, gobernar el SII significaba tomar decisiones sobre cómo se gestionan las informaciones, cómo se tratan los datos incorporados al canal y en qué momentos procede remitirlas a órganos internos o externos. Todas estas decisiones influyen directamente en los fines y medios del tratamiento, aspecto clave del análisis de incompatibilidad según las Directrices del antiguo Grupo de Trabajo del Artículo 29 (WP243) y la doctrina del Tribunal de Justicia de la Unión Europea (asunto C-453/21).

b) El DPD no puede supervisar lo que también gestiona. El RGPD exige que el DPD mantenga una posición neutral y supervisora, actuando como garante de cumplimiento. Si, al mismo tiempo, es quien gestiona operativamente un tratamiento (como el canal interno), su facultad de supervisión queda anulada. La AEPD lo resume de forma clara: el DPD no puede ser juez y parte dentro del mismo sistema de tratamiento. Esta incompatibilidad se agrava al tratarse de un sistema que implica datos especialmente sensibles y decisiones de intervención disciplinaria o legal. Asimismo, la AEPD trae a colación el literal del artículo 8.4 de la Ley 2/2023, precepto que establece lo siguiente: "El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, no podrá recibir instrucciones de ningún tipo en su ejercicio, y deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo".

c) Falta de garantías y ausencia de análisis previo. La Agencia recuerda que es responsabilidad exclusiva de la organización, no del DPD, acreditar que las funciones adicionales no generan conflicto de intereses. Esto exige un análisis previo, documentado y basado en criterios objetivos. La Diputación no realizó ese análisis y tampoco estableció salvaguardas internas (por ejemplo, reglas de abstención, límites funcionales, separación de accesos) que hubieran permitido evaluar y, en su caso, mitigar el riesgo. Esta ausencia de medidas es decisiva para concluir que se vulneró el artículo 38 RGPD.

d) Independencia material versus independecnia formal. La AEPD rechaza la idea de que la independencia del DPD pueda garantizarse únicamente con elementos formales, como reportar al más alto nivel jerárquico o no tener voto en ciertos comités, si en la práctica, desempeña funciones que lo sitúan dentro del circuito operativo que debe auditar. La independencia, recuerda la Agencia, es material, práctica y verificable, no declarativa.

Cabe mencionar que la AEPD recuerda en la referida resolución que "Ante la cuestión planteada por el propio DPD sobre la posible incompatibilidad, se formuló consulta a la AEPD, manteniendo la designación de la DPD en tanto se recibía la contestación. Dicha consulta fue resuelta el 25 de febrero de 2025, concluyendo que no era posible asignar funciones de responsable del sistema interno de información al DPD".

Es decir, la AEPD ya se había pronunciado al respecto sobre este caso especifico, concluyendo en una consulta previa que mantener ambos roles sobre la misma persona generaba una incompatibilidad en los términos establecidos en la normativa aplicable.

Por último, resulta preciso traer a colación las referencias realizadas tanto por la Diputación como por la AEPD al informe 2018-0170[2] de esta última en el que se analizó la compatibilidad entre el DPD y el Responsable de Seguridad en el ámbito del Esquema Nacional de Seguridad, en el que -resumidamente- se concluyó que, con carácter general, debe existir la necesaria separación entre el delgado de protección de datos regulado en el RGPD y el responsable de seguridad del ENS, sin que sus funciones puedan recaer en la misma persona u órgano colegiado, pudiendo recaer sobre la misma persona únicamente en el caso de organizaciones de pequeño tamaño y/o escasez de recursos adoptando las medidas técnicas y organizativas necesarias para evitar posibles conflictos de interés que pudieran presentarse en el ejercicio de sus respectivas funciones.

## 3. Conclusión

A modo de conclusión, se puede indicar que la resolución de la AEPD ofrece un criterio claro sobre la importancia de contar con medidas preventivas sólidas y asegurar que el Delegado de Protección de Datos mantiene una independencia real en el desempeño de sus funciones.

El caso demuestra que ciertas acumulaciones de roles pueden generar incompatibilidades no siempre evidentes a primera vista, especialmente cuando implican tareas operativas o decisorias y que, realizando el análisis adecuado previo, así como la adopción de medidas adecuadas que permitan garantizar la adecuada gestión del conflicto de intereses, puede ser factible la compatibilidad de las funciones de uno y otro.

La interpretación de la AEPD refuerza la necesidad de revisar la arquitectura interna de cumplimiento y de documentar adecuadamente la asignación de funciones, con el objetivo de garantizar un modelo de gobernanza que sea sólido, transparente y alineado con el RGPD. Al mismo tiempo, la Agencia recuerda que este tipo de situaciones debe valorarse mediante un análisis de las funciones detallado y estudiarse caso por caso, atendiendo a las particularidades de cada organización y al alcance real de las funciones desempeñadas.

Lo anterior se puede traducir en que, como norma general, la figura del Delegado de Protección de Datos no puede ser asumida por el Responsable del Sistema Interno de Información y viceversa, salvo que quede debidamente acreditado y justificado el análisis realizado sobre la falta de medios y de recursos, la posible incompatibilidad existente y los mecanismos desplegados para evitar que la asunción de ambos roles interfiere en su correcto funcionamiento.

Por último, debe tenerse claro que la AEPD no manifiesta en ningún momento la existencia de incompatibilidad entre la función del Compliance Officer y del DPD, siendo el Compliance Officer una figura completamente diferente al responsable del canal de información o denuncias. Si bien son dos puestos que podrían entrar en conflicto puntualmente, dicho conflicto podría ser debidamente gestionado adoptando las medidas y controles de carácter material adecuados, en la medida en que ambas dos funciones se ejercen en la segunda línea de defensa.

Área de Protección de Datos de ECIJA
info@ecija.com
Telf.: + 34 91.781.61.60

[2] El texto completo del informe puede consultarse en el siguiente enlace: https://www.aepd.es/documento/2018-0170.pdf