# Resolución AEPD 00331/2022: Incumplimiento del principio de privacidad desde el diseño y por defecto, y de la seguridad del tratamiento. [1]

**Fecha: 2 de octubre de 2023.**

El objeto de la presente nota es el análisis de los criterios jurídicos apreciados por la Agencia Española de Protección de Datos (en adelante, "**AEPD**" o la "**Agencia**") en la Resolución del Procedimiento Sancionador 00331/2022, de fecha 28 de julio de 2023, la cual impone una **sanción de 2,5 millones de Euros por infracción de los artículos 25 y 32 del Reglamento General de Protección de Datos (RGPD)** – 1 millón de Euros por falta de implementación de medidas de seguridad adecuadas al riesgo y 1,5 millones de Euros por el incumplimiento del principio de privacidad desde el diseño y por defecto–, a la entidad financiera Openbank S.A. (en adelante, "**Openbank**").

## (I) Supuesto de hecho

Se admitió a trámite la reclamación presentada por un cliente de Openbank, a quien esta entidad había solicitado que aportara documentación que declarara el origen de varias cantidades recibidas en su cuenta bancaria, siguiendo las directrices señaladas por la Ley de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo (en adelante, la **"LPBCFT"**), y por su Reglamento de desarrollo, vía correo electrónico. En concreto, el cliente presentó la reclamación después de haber solicitado a la entidad un mecanismo alternativo al correo electrónico para remitir la información requerida, el cual permitiera enviar la documentación a través de un canal seguro.

## (II) Análisis jurídico

- **Sobre el cumplimiento del principio de protección de datos desde el diseño (artículo 25 RGPD)**

La AEPD ha concluido que Openbank no cumplió con el principio de privacidad desde el diseño y por defecto por diversas razones:

- No **prever, evaluar ni diseñar correctamente y de forma previa** el tratamiento consistente en la remisión de documentación por parte del interesado requerida en virtud del Capítulo II de la LPBCFT, máxime cuando en los documentos aportados por Openbank se calificaba el riesgo inherente de dicho tratamiento como de alto impacto. Por ello, no se han aplicado las medidas correspondientes para aplicar efectivamente los principios del tratamiento y, especialmente, el de confidencialidad.

- No prever la posibilidad de que los clientes enviaran la información requerida por un **medio seguro**, considerando el ciclo de vida del tratamiento, y teniendo en cuenta

que ya existían implementados otros métodos alternativos de proporcionar información por parte de los clientes en la entidad.

A tal efecto, la Agencia advierte que el cumplimiento del principio de privacidad desde el diseño no **se agota con la realización de una EIPD,** sino que deben implementarse las medidas adecuadas atendiendo a los resultados obtenidos en la evaluación del tratamiento.

Por otra parte, la Agencia especifica que, ante una comunicación dirigida por un interesado, solo se considerará cumplido este principio si se modifican, tanto la evaluación de los riesgos previamente realizada, como las medidas técnicas y organizativas correspondientes.

En este mismo sentido, de acuerdo con la falta de respuesta al reclamante por parte de Openbank, la AEPD resalta la necesidad de establecer procedimientos internos a fin de canalizar cuestiones que versen sobre protección de datos.

- **Sobre la vulneración del artículo 32 del RGPD.**

La AEPD fundamenta la vulneración de la obligación de implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en varios aspectos:

- El envío de la información solicitada en virtud del Capítulo II de la LPBCFT mediante correo electrónico **no era un medio adecuado ni seguro** en función del riesgo que podía existir para los derechos y libertades de los interesados y exigía la adopción de medidas reforzadas por su alto impacto.

- **Delegar la seguridad del correo electrónico en los proveedores** de esta tecnología o **hacer depender la seguridad del nivel de conocimientos técnicos del propio cliente** - sin asistirles en dicho proceso- y de que tenga las herramientas adecuadas para ello, supone una transferencia del riesgo y responsabilidad de Openbank al cliente que no se ajusta al cumplimiento del principio de responsabilidad consagrado en la normativa de aplicación.

- La vulneración relacionada con la implementación de medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo **se diferencia de las medidas técnicas y organizativas** exigidas en virtud del artículo 25, puesto que estas últimas – al contrario que las establecidas en el artículo 32– no están dirigidas específicamente a la seguridad, sino a garantizar el cumplimiento normativo de todo el RGPD.

- **Sobre si la información solicitada por la entidad tiene consideración de datos financieros.**

La AEPD considera que toda la documentación relacionada con el origen de los fondos y movimientos en cuentas bancarias solicitada a la parte reclamante por Openbank contiene datos relacionados con la situación económica y el estado financiero de los clientes.

Estos datos permiten determinar la situación financiera o la solvencia patrimonial de una persona, por lo que requieren de una mayor protección (la AEPD habla de *medidas reforzadas*) en atención a los riesgos en los derechos y libertades de los interesados, independientemente de que sean o no considerados datos sensibles.

Además, la Agencia señala que la obligación de adoptar la protección de datos desde el diseño y por defecto, así como la obligación de contar con las medidas de seguridad apropiadas en función del riesgo para los derechos y libertades debe cumplirse con independencia de la naturaleza de los datos. No obstante, dada su especial protección, la Agencia considera que debe aplicarse este hecho como agravante, en virtud del artículo 83 RGPD.

## (III) Conclusión

En definitiva, sin perjuicio de otras particularidades indicadas por la AEPD en este procedimiento, relacionadas con el ámbito competencial de la agencia en asuntos relacionados con la prevención del blanqueo de capitales, el principio de proporcionalidad o el régimen sancionador, cabe destacar específicamente cómo la AEPD viene a delimitar las exigencias derivadas del cumplimiento del principio de privacidad desde el diseño y por defecto, diferenciándolo de la obligación que dispone el artículo 32 del Reglamento. En este sentido, si bien en ambos casos se establece la necesidad de establecer medidas técnicas y organizativas, estas suponen obligaciones diferenciadas e independientes, tienen elementos dispares y finalidades distintas que deben ser tenidas en cuenta por los responsables y los encargados del tratamiento.

Quedamos a su disposición para cualquier duda o cuestión que pudiera surgir.

Reciba un cordial un saludo,

**Área de Protección de Datos de ECIJA**

info@ecija.com

Telf: + 34 91.781.61.60

[1] https://www.aepd.es/es/documento/ps-00331-2022.pdf